Stratus® ftServer® System Administrator's Guide for the Windows Operating System

Stratus Technologies
R014W-12

Notice

The information contained in this document is subject to change without notice.

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF STRATUS TECHNOLOGIES, STRATUS MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE. Stratus Technologies assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document.

Software described in Stratus documents (a) is the property of Stratus Technologies Bermuda, Ltd. or the third party, (b) is furnished only under license, and (c) may be copied or used only as expressly permitted under the terms of the license.

Stratus documentation describes all supported features of the user interfaces and the application programming interfaces (API) developed by Stratus. Any undocumented features of these interfaces are intended solely for use by Stratus personnel and are subject to change without warning.

This document is protected by copyright. All rights are reserved. No part of this document may be copied, reproduced, or translated, either mechanically or electronically, without the prior written consent of Stratus Technologies.

Stratus, the Stratus logo, ftServer, the ftServer logo, Continuum, StrataLINK, and StrataNET are registered trademarks of Stratus Technologies Bermuda, Ltd.

The Stratus Technologies logo, the Continuum logo, the Stratus 24 x 7 logo, ActiveService, ftScalable, and ftMessaging are trademarks of Stratus Technologies Bermuda, Ltd.

All other trademarks are the property of their respective owners.

Manual Name: *Stratus ftServer System Administrator's Guide for the Windows Operating System*

Part Number: R014W
Revision Number: 12
Software Release Number: ftServer System Software for the Windows Operating System, Release 6.0.0
Publication Date: August 2009

Stratus Technologies, Inc.
111 Powdermill Road
Maynard, Massachusetts 01754-3409

© 2009 Stratus Technologies Bermuda, Ltd. All rights reserved.

Contents

Preface xi

1. Introduction to System Administration 1-1
- System Administration Tools 1-1
  - Active Upgrade 1-1
  - ftSys Management Console 1-2
  - ActiveService Network 1-2
  - Virtual Technician Module Console 1-3
  - Disk-Management Tools 1-3
- System Software Features 1-4
  - Fail-Safe Software 1-4
  - Stratus Services 1-4
  - Open Driver Architecture 1-4
  - Rapid Disk Resync Disk Mirroring 1-5
- Initial Configuration 1-6
- Documentation 1-6
  - Online Documentation 1-6
  - Stratus Help System 1-7
- Windows Documentation 1-7

2. Operating and Monitoring Your System 2-1
- Starting Up and Shutting Down A System 2-2
  - Enabling the Power Button on the Machine 2-2
  - CPU Element Resynchronization 2-3
  - Managing CPU Element Bringup 2-4
- Controlling the Modem 2-4
- Accessing Your System Desktop Remotely 2-5
  - Enabling Remote Desktop 2-5
  - Running ftSMC Remotely 2-6
  - Booting or Shutting Down a System Through VTM Console 2-6
- Using the VTM 2-6
  - Setting Up a VTM Administrator Account 2-6
  - Logging in to the VTM Console 2-7

Configuring Static IP Addresses for the VTM Network Ports 2-7
Using Windows System Event Logs 2-8
Starting Computer Management 2-8
Setting the Size of Event Log Files 2-9
Saving Event Log Files 2-9
Monitoring ftServer Services 2-10
Managing BIOS Settings 2-11
Determining the BIOS Version 2-12
Writing to DVD-RWs on Windows Server 2003 Systems 2-12
Understanding Floppy Disk Drive Volume Letters 2-12
Using Serial Ports 2-13
Understanding Uninterruptible Power Supplies 2-13
Maintaining System Power During a UPS Failure 2-14
Changing the IP Address of Systems with a UPS 2-14
Understanding SNMP Traps 2-14
Understanding Updates and Hotfixes 2-15
Avoiding Problems 2-15

3. ftSys Management Console 3-1
ftSMC Overview 3-1
Running ftSMC 3-2
Running ftSMC Directly on Your ftServer System 3-2
Running ftSMC on a Remote System 3-2
Adding the ftSMC Snap-in to MMC on a Windows Server system 3-3
Opening a Previously Saved MMC Console 3-5
Performing ftSMC Tasks 3-6
ftSMC Interface 3-6
Details Pane 3-7
Icons Used in ftSMC 3-8
Refreshing the ftSMC Display 3-10
Viewing and Changing Properties 3-11
Required Operational States for Commands 3-12
CPU and I/O Enclosures and Elements 3-12
Primary and Secondary CPU-I/O Enclosures 3-12
Switching the Primary CPU-I/O Enclosure 3-13

4. Disk Storage Management 4-1
Data Fault Tolerance 4-1
Guidelines for System Disks 4-2
Using RDR for Mirroring and Fault Tolerance 4-2
Automatic Virtual Disk Expansion 4-3

Managing RDR Disks 4-4
Creating a First RDR Virtual Disk 4-5
Mirroring Disks Using RDR 4-6
RDR Disk Numbering 4-6
Adding a Physical Disk to an RDR Virtual Disk 4-7
Disk Failures During Resynchronization 4-10
Write Caching 4-10
Setting the Cache Flush Interval 4-11
Read-load (LUN Load) Balancing 4-11
Mirroring Dynamic Disks with RDR 4-12
Setting the Active RDR Disk (Plex) 4-12
Deleting the RDR Configuration on a Physical Disk 4-13
Changing Automount Behavior 4-14
Removing a Physical Disk from an RDR Virtual Disk 4-14
Deporting a Physical Disk from an RDR Virtual Disk 4-15
Creating a Spare Bootable RDR Disk 4-16
Breaking a Physical Disk from an RDR Virtual Disk 4-17
Setting or Clearing the MTBF for Disks 4-17
Setting the Hard MTBF Threshold 4-18
Setting the MTBF Faultcount Limit 4-18
Setting the Soft MTBF Threshold 4-19
Clearing MTBF Settings 4-19
Booting a System with a Backup RDR Boot Disk 4-20
Reusing Data Disks 4-20
Reusing a Stored-Data Disk 4-20
Removing the RDR Configuration from a Stored-Data Disk 4-20
Resynchronizing RDR Disks 4-21
Using Resynchronize This Physical Disk From RDR Virtual Disk 4-22
Using Resynchronize Physical Disks Of This RDR Virtual Disk 4-22
Resynchronizing a Backup Boot RDR Disk 4-22
Recovering and Replacing RDR Disks 4-23
Verifying RDR Disks 4-23
Making Sure You Do Not Boot from a Stale Disk 4-24
Configuring the Priority of RDR Virtual Disk Resynchronization 4-25
Using Volume Mirroring for Fault Tolerance 4-25
Mirrored Volume Resynchronization 4-26
Volume Resynchronization After Rebooting 4-26
Using Hardware RAID Controllers For Fault Tolerance 4-27
ftSMC Interface for Storage Enclosures and Subsystems 4-27
Storage Enclosure Node 4-27
Slot Node 4-28

Disk Node 4-28
ftScalable Storage 4-28
EMC Attached Storage 4-28
Mirroring Disks in ftScalable Storage Systems 4-29
Finding an Internal Physical Disk 4-29
Finding an External Physical Disk 4-31

5. Troubleshooting 5-1
MTBF Statistics 5-2
Clearing the MTBF 5-2
Changing the MTBF Threshold 5-2
Taking Components Offline and Bringing Them Online 5-3
Expansion ROM Console Message During System Boot 5-3
Hard Disks 5-3
Recovering a Disk 5-3
Replacing a Failed Disk in Windows Disk Management 5-4
Replacing a Failed Disk with an Uninitialized Disk 5-4
Replacing a Failed Disk with an Initialized Disk 5-5
Hardware Installation Wizard 5-5
Determining That a Component Has Failed 5-6
Using LEDs to Troubleshoot Hardware 5-6
Using ftSMC to Troubleshoot Hardware 5-6
Locating Components 5-7
Device IDs and Device Paths 5-7
Diagrams of Component Locations 5-8
System Elements and Internal Storage Disk Locations 5-8
When Windows Does Not Respond 5-9
Delayed System Restart 5-9
Unresponsive Mouse and Keyboard 5-9
Remote Event Notification and Service 5-10
Remote Reporting of Events 5-10
Alarm Messages 5-10
Event Notification on Boot Failure 5-11
System Inventory Reports 5-11
Event-Log Entries 5-11
Remote Service 5-11
Making Dump Files 5-12
Using the NMI (Dump) Button 5-12
Configuring System Memory Dumps 5-13
Dump and Go 5-13
Making a Dump File Using the VTM Console 5-14

Disaster Recovery 5-14
Safe Mode 5-14
Booting From a Spare System Disk 5-15
Windows Hotfixes Distributed by Stratus 5-16
Adaptec SAS Controller BIOS RAID Option 5-17
Tape Drives and Backup on Windows Server 2008 Systems 5-17

Appendix A. Advanced Topics A-1
Using Windows Headless Mode and Console Redirection A-1
Enabling Multiple Login Sessions (Windows Server 2008) A-2

Appendix B. Configuring And Managing Ethernet PCI Adapters B-1
Using Device Manager to Manage Ethernet Adapters B-2
Fixing Duplicate Network Adapter Names B-2
Fault-Tolerant Ethernet Teams and IP Multicasting B-3
Virtual LANs B-4
Configuring Ethernet Teams B-5
Locating Ethernet PCI Adapters B-6
Configuring Link Speed and Duplex Mode B-7
Creating Ethernet Teams B-10
Disabling Receive Load Balancing B-11
Designating Primary and Secondary Adapters B-12
Configuring Virtual LANs Over a Team B-14
Verifying the Configuration of Teams and VLANs B-16
Assigning an IP Address to a Team or VLAN B-18
Managing Ethernet Teams B-21
Removing Ethernet PCI Adapters from a Team B-21
Physically Replacing Removed Adapters B-23
Adding Ethernet PCI Adapters to a Team B-24
Updating a Team's Ethernet Address B-25
Removing an Ethernet Team B-28
Using Diagnostics B-29
Using ftSMC to Check Network Statistics B-30
Renaming Ethernet Teams B-31

Index Index-1

Figures

Figure 3-1.	ftSMC Tree	3-5
Figure 3-2.	ftSMC User Interface	3-7
Figure 3-3.	Using What's This? in the Details Pane	3-8
Figure 3-4.	System Inventory Icons	3-8
Figure 3-5.	Simplexed Icon for Invalid Configuration	3-9
Figure 3-6.	Warning and Error Icons	3-10
Figure 3-7.	Warning and Inventory Error Icons	3-10
Figure 3-8.	Threshold Warning Icon	3-10
Figure 3-9.	ftSMC Details Pane Refresh Options	3-11
Figure 3-10.	Properties Command in Shortcut Menu	3-11
Figure 5-1.	Warning and Error Icons	5-6
Figure 5-2.	Component Levels	5-7
Figure 5-3.	CPU-I/O Enclosure and Disk Slot Labeling	5-9
Figure B-1.	Identify Adapter Dialog Box	B-7
Figure B-2.	Setting the Link Speed and Duplex Mode	B-9
Figure B-3.	Naming the New Team	B-10
Figure B-4.	Network Adapters in Device Manager	B-12
Figure B-5.	Assigning Priorities to Ethernet PCI Adapters	B-13
Figure B-6.	Adding a VLAN to a Team	B-14
Figure B-7.	Specifying a VLAN ID and Name	B-15
Figure B-8.	Finding a Team's IP Address in Windows 2003	B-17
Figure B-9.	Finding a Team's IP Address in Windows 2008	B-17
Figure B-10.	Ethernet Team Properties on a Windows Server 2003 System	B-18
Figure B-11.	Ethernet Team Properties on a Windows Server 2003 System	B-19
Figure B-12.	Internet Protocol (TCP/IP) Properties	B-20
Figure B-13.	Removing an Ethernet PCI Adapter from a Team	B-22
Figure B-14.	Confirmation Message: Removing an Ethernet PCI Adapter from a Team	B-22
Figure B-15.	Icon for a Missing (Removed) Adapter	B-24
Figure B-16.	Obtaining the Team Ethernet Address	B-26
Figure B-17.	Updating the Team Ethernet Address	B-27
Figure B-18.	Removing a Team of Ethernet PCI Adapters	B-28
Figure B-19.	Confirmation Message: Removing a Team	B-29
Figure B-20.	Diagnostics	B-30
Figure B-21.	Network Statistics in ftSMC	B-31

Tables

Table 3-1.	ftServer System Models by P-Package	3-1
Table 3-2.	ftSMC User Interface Key Elements	3-7
Table 3-3.	ftSMC Warning and Error Icons	3-9
Table 3-4.	Operational State for Associated Commands	3-12
Table 4-1.	RDR Disk Numbering	4-7
Table 4-2.	FC Host Bus Adapter State and Reason Property Values	4-29
Table 5-1.	System Device IDs	5-8

Preface

Purpose of This Manual

The *Stratus ftServer System Administrator's Guide for the Windows Operating System* (R014W) documents tasks and information for system administrators of ftServer 2600, 4500, and 6300 systems.

Audience

This manual is intended for anyone who administers or troubleshoots ftServer 2600, 4500, and 6300 systems.

Revision Information

This manual is a revision. This revision incorporates support for ftServer System Software (ftSSS) for the Windows Operating System, Release 6.0.0, on ftServer 2600, 4500, and 6300 systems.

As of ftSSS for the Windows Operating System, Release 6.0.0, information about POST codes appears only in the *Stratus ftServer Virtual Technician Module User's Guide* (R642).

Notation Conventions

This document uses the notation conventions described in this section.

Warnings, Cautions, and Notes

Warnings, cautions, and notes provide special information and have the following meanings:

WARNING

A warning indicates a situation where failure to take or avoid a specified action could cause bodily harm or loss of life.

CAUTION

A caution indicates a situation where failure to take or avoid a specified action could damage a hardware device, program, system, or data.

NOTE

A note provides important information about the operation of an ftServer system.

Typographical Conventions

The following typographical conventions are used in ftServer documents:

- The bold font emphasizes words in text or indicates text that you type, the name of a screen object, or the name of a programming element. For example:

  Before handling or replacing system components, make sure that you are properly grounded by using a grounded wrist strap.

  In the **System Properties** dialog box, click the **Hardware** tab.

  Call the **RegisterDeviceNotification** function.

- The italic font introduces new terms and indicates programming and command-line arguments that the user defines. For example:

  Many hardware components are *customer-replaceable units* (CRUs), which can be replaced on-site by system administrators with minimal training or tools.

  copy *filename1 filename2*

  Pass a pointer for the *NotificationFilter* parameter

- The monospace font indicates sample program code and output, including message text. For example:

```
#include <iostream.h>

The operation completed successfully.
```

Getting Help

If you have a technical question about ftServer system hardware or software, try these online resources first:

- **Online support from Stratus Customer Service.** You can find the latest technical information about an ftServer system through online product support at the Stratus Technical Support Website.
- **Online product support for Microsoft® products**. Your primary source for support is the computer manufacturer who provided your software, or an authorized Microsoft Support Provider. You can also find the latest technical information about Microsoft Windows® and other Microsoft products through online product support at the Microsoft Help and Support Website.

If you are unable to resolve your questions with the help available at these online sites, and the ftServer system is covered by a service agreement, please contact the Stratus Customer Assistance Center (CAC) or your authorized Stratus service representative. Your system administrator may have configured a Stratus Support phone number in ftSys Management Console (ftSMC), a snap-in to Microsoft Management Console (MMC). In ftSMC, under **ftServer Configuration**, click **ActiveService Network** to display the node's properties in the ftSMC details pane. The properties include a **Stratus Support Phone** item. The value of this property, if configured, is a telephone number you can call for support.

Chapter 1
Introduction to System Administration

The following topics provide an introduction to Stratus ftServer 2600, 4500, and 6300 system administration.

- "System Administration Tools" on page 1-1
- "System Software Features" on page 1-4
- "Initial Configuration" on page 1-6
- "Documentation" on page 1-6
- "Windows Documentation" on page 1-7

Features of ftServer software further support system fault-tolerance for properly configured systems.

If you have a service contract, Stratus or an authorized Stratus service representative provides continuous, remote, system monitoring and diagnosis for ActiveService Network (ASN) management.

Disk-management tools are also available on your ftServer system.

System Administration Tools

System administration tools enable you to monitor system performance and system-component status, diagnose errors, and identify failed components. Using the tools, you can take failed components offline and put replacement components online.

These features include Active Upgrade, ftSys Management Console (ftSMC), ActiveService Network (ASN), Virtual Technician Module (VTM) console, and disk-management tools.

Active Upgrade

Optional Active Upgrade™ technology enables you to upgrade your system and application software with minimal downtime.

Instead of taking your system offline to run upgrade procedures, you can use the Active Upgrade process to split the system into two independently-running systems, one

"side" of which you upgrade while the other side continues to run your applications without interruption. See the *Stratus ftServer: Active Upgrade User's Guide* (R017W) or the Active Upgrade online help for more information.

ftSys Management Console

The ftSys Management Console (ftSMC) is a graphical user interface that enables you to monitor and manage your system's fault-tolerant software and hardware. See Chapter 3 for details.

ActiveService Network

Your ftServer system offers an optional, secure network, the ActiveService Network (ASN). ASN enables the CAC or your authorized Stratus service representative to provide remote monitoring, diagnosis, troubleshooting, and problem-resolution services to your systems 24 hours a day, 7 days a week. Access to the ASN requires a service contract with Stratus or an authorized Stratus service representative and is implemented across a modem or over the Internet.

Having ASN connectivity enables:

- Your system to send alerts (call-home alarm messages) to the CAC or your authorized Stratus service representative when unusual events occur on the system
- The CAC or your authorized Stratus service representative to access the system through a connection to the ASN

Your system can connect to the ASN through:

- A modem connected to the system
- The Internet
- The VTM console or an ftGateway system

NOTE

An ftServer 2600, 4500, or 6300 system running ftSSS for the Windows Operating System, Release 6.0.0, provides only ftGateway slave support and cannot serve as an ftGateway master. For ftGateway master support, use an ftServer system that runs a version of ftSSS for the Windows Operating System, Release 5.3.

Internet-based ASN connects over a secure path to your authorized Stratus service representative.

After verifying a hardware problem, your authorized Stratus service representative can send out a replacement CRU.

See the *Stratus ActiveService Network Configuration Guide* (R072) for more information, and online help for ftSys Management Console (ftSMC) for instructions in how to configure ASN alarm notification by email.

Virtual Technician Module Console

The Virtual Technician Module (VTM) console is a Web-based console that enables you, the CAC, or your authorized Stratus service representative to control, monitor, and diagnose the system. You can access the VTM console over a LAN, or the Internet, if Internet connectivity is available. You can use the VTM console even if the host system's operating system is unresponsive and its network connections are lost. VTM console functionality also includes:

- Remote Keyboard, Video, Mouse (KVM) support
- Access to attached storage
- Diagnosis of a system that is powered off (however, standby power must be available)
- Power-cycling of a system

Remote KVM Console enables you to manage the host computer remotely over the Web-based console. Using Remote KVM Console, you can view the remote system desktop and redirect its local keyboard and mouse.

A VTM requires assignment of two IP addresses, either static or from a Dynamic Host Configuration Protocol (DHCP) server. See "Configuring Static IP Addresses for the VTM Network Ports" on page 2-7.

Disk-Management Tools

Disk-management tools enable you to monitor disk status, mirror entire physical disks, create logical volumes, mirror volumes across multiple disks, and perform other data-storage operations.

See also "Rapid Disk Resync Disk Mirroring" on page 1-5.

System Software Features

ftServer System Software has features designed to support fault-tolerant operation and high availability. These features include fault-tolerant, fail-safe software, Stratus services, open architecture drivers, and Rapid Disk Resync disk mirroring.

NOTE

ftServer 2600, 4500, and 6300 systems do not support the Windows Server 2008 BitLocker Drive Encryption feature.

Fail-Safe Software

ftServer System Software works in conjunction with lockstep technology to increase system reliability. Fail-safe software features capture issues and report them to the CAC or your authorized Stratus service representative. Even data in memory can be constantly protected and maintained.

Stratus's hardened device drivers prevent software failures, and Stratus provides an embedded open-driver technology that enables third-party device drivers to access hardening capabilities.

Stratus Services

Stratus provides software fault-tolerant services that run on your system as Windows-based services. These services constantly monitor for, and respond to, hardware problems. Applications do not need customization to support the services.

These services start automatically when the system boots and remain running during normal operation. If a situation requires system administrator intervention, you can use Computer Management to manually start and stop system services. See "Monitoring ftServer Services" on page 2-10 for details.

See the *Stratus ftServer Systems: Technical Reference Guide* (R550) for descriptions of the Stratus services.

Open Driver Architecture

Your ftServer system supports both vendor-supplied drivers and Stratus-supplied drivers for PCI adapters. ftServer systems support vendor-supplied drivers for the PCI adapters that you supply. For PCI adapters that Stratus provides, Stratus supplies drivers that it has enhanced with support for surprise removal.

In addition, your ftServer system uses other drivers developed by Stratus. These drivers allow the system and all PCI devices to integrate with the ASN, and provide management of all system devices and device fault-tolerance.

ASN integration provides:

- Automatic reporting of device failures to the CAC or your authorized Stratus service representative
- Notification to you by the CAC or your authorized Stratus service representative when a device fails
- Inventory reporting to the CAC or your authorized Stratus service representative that lists all PCI devices in the system
- Comprehensive debug information about all devices in the system for use by the CAC or your authorized Stratus service representative in troubleshooting your system

Management of PCI devices includes:

- On your ftServer system, hot-plug support alerts the plug-and-play manager to bring a device into service or take it out of service. You can initiate bring-up or bring-down from ftSMC. Hot-plug support also initiates discovery of newly attached or removed devices.

  NOTE

  You must remove the CPU-I/O enclosure from the system in order to remove a PCI adapter.

- Display of information so that you know whether removing a device will compromise the system. The drivers can set LEDs and values in ftSMC that let you know whether you can safely remove a component.

Display of information in ftSMC about a device's fault-tolerance, including:

- Automatic restart of failed devices. The device will be restarted after transient faults, until it falls below its mean-time-between faults (MTBF) threshold.
- Tracking the MTBF of a device and management of the device when it experiences faults. You can set parameters to take the device out of service when the device experiences an unacceptable MTBF. You can configure the rules for MTBF management.

Rapid Disk Resync Disk Mirroring

Rapid Disk Resync (RDR) disk-mirroring technology provides faster resynchronization of mirrored disks than other mirroring methods after transient failures or when a single disk is briefly removed from service. For optimal performance, use RDR to mirror disks in internal storage.

Initial Configuration

Configure the following items before you use your system:

- **System software**. See the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) guide for software installation and configuration details.
- **Disk storage.** Create a backup system disk and mirror the disks in your system. If you are implementing RDR disk mirroring, see the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) guide for details. If you are implementing volume mirroring, see your disk-management tool documentation.
- **Network connections**. Configure Ethernet adapters in teams to achieve increased throughput and fault tolerance. In a team, one adapter is primary and the other adapters in the team are secondary. See the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) and Appendix B for details about configuring Ethernet adapter teams.
- **Uninterruptible power supply (UPS).** See your system's hardware installation guide for information about connecting a UPS to a system. See the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) for information about how to configure a UPS for use with your system.
- **ASN.** If you have purchased remote diagnostic, troubleshooting, and problem-resolution services from the CAC or your authorized Stratus service representative, configure the Stratus ASN. See the *Stratus ActiveService Network Configuration Guide* (R072) for details.

Documentation

The *Stratus ftServer 2600, 4500, and 6300 Systems: Site Planning Guide* (R638) lists ftServer system documentation. You can find additional information in ftSMC Help.

Online Documentation

The **ftServer Help and Manuals** folder on the ftServer desktop contains links to the Stratus ftServer documents.

You can view the documents in the Help system or open them in PDF format for viewing or printing.

To gain access to the documents on the World Wide Web, point your browser to the ftServer StrataDOC Web site (http://stratadoc4ftserver.stratus.com).

Stratus Help System

The Stratus Help system consists of the following:

- **General Help.** You can access general help from the **ftServer Help and Manuals** icon on the desktop, the **Help** button on an application's menu bar, or by pressing the **F1** key.
- **Context-Sensitive Help.** Context-sensitive help is available for certain items within help-enabled applications (such as the ftSMC snap-in). To access this help, select an icon in the ftSMC system inventory tree and press F1. Alternatively, right-click an ftSMC system inventory tree icon, and in the shortcut menu, click **Help**.
- **What's This? of ftSMC Help.** What's This? of ftSMC Help is available for items in the details pane of the ftSMC snap-in. To access it, right-click the question mark (**?**) icon in front of the item, and in the shortcut menu, click **What's this?** (see Figure 3-3 for an example). What's This? help is also available from certain dialog boxes having the What's this? help icon (**?**) in their upper-right corner. For example, in a **Properties** dialog box in ftSMC, click the help icon (**?**), then click a box, and a pop-up window of ftSMC Help is displayed.

Windows Documentation

This manual documents only those system administration tasks that are required for ftServer systems in particular, not those that are required for Windows-based servers in general. General system-administration tasks for Windows systems include:

- Configuring networks and managing access to network resources
- Configuring Windows services
- Configuring domain controllers
- Implementing and managing Active Directory
- Setting up user accounts and managing users
- Setting up and configuring printers
- Managing server security
- Backing up and restoring data

For help with these kinds of tasks, see the associated Microsoft Help system and the Windows OS documentation provided by Microsoft.

Chapter 2
Operating and Monitoring Your System

For information about system operation, see the following topics:

- “Starting Up and Shutting Down A System” on page 2-2
- “Controlling the Modem” on page 2-4
- “Accessing Your System Desktop Remotely” on page 2-5
- “Using the VTM” on page 2-6
- “Using Windows System Event Logs” on page 2-8
- “Monitoring ftServer Services” on page 2-10
- “Managing BIOS Settings” on page 2-11
- “Writing to DVD-RWs on Windows Server 2003 Systems” on page 2-12
- “Understanding Floppy Disk Drive Volume Letters” on page 2-12
- “Using Serial Ports” on page 2-13
- “Understanding Uninterruptible Power Supplies” on page 2-13
- “Understanding SNMP Traps” on page 2-14
- “Understanding Updates and Hotfixes” on page 2-15
- “Avoiding Problems” on page 2-15

Starting Up and Shutting Down A System

For normal system startup and shutdown, and to completely remove power from the system, see the operation and maintenance guide for your system.

CAUTION

Always shut down the operating system before turning the system power off.

NOTES

1. **Give the system time to recover automatically from problems.** If the system hangs for any reason while it is booting, wait at least ten minutes before intervening manually.
2. If a system contains failed components, it may attempt to boot for an extended period of time. This is because the system makes up to six attempts to boot, each time trying with a different combination of components. You can monitor the boot process on the screen or in a VTM console session.

You can accomplish an orderly shutdown of the system from a remote computer by accessing the Windows desktop and executing a **Shut Down** command.

You must physically be at the system to see the message indicating that it is safe to power off the system. To turn off power, use the power button on the machine, the standby circuit-breaker switches, or the VTM console. Note, however, that the Windows Shut Down command automatically powers down the system.

Enabling the Power Button on the Machine

The power button on the machine performs an orderly shutdown when pressed once. However, if no one is currently logged on to the system, the power button may not work properly on all versions of the Windows operating system. You may have to enable the power button on the machine to operate correctly in the event that no one is logged onto a system.

To enable the power button on the machine to shut down a system onto which no one has yet logged, enable the following Windows Security option:

Shutdown: Allow system to be shutdown without having to log on

To set the shutdown option on a Windows Server 2003 system

1. Refer to the Windows Help topic **Opening the Local Group Policy Editor**
2. Follow the instructions for a **Local Computer** or a **Group Policy object**.

To set the shutdown option on a Windows Server 2008 system

1. Click **Start**, **Administrative Tools**, and **Local Security Policies**.
2. Under **Security Settings**, expand **Local Policies**, and double-click **Security Options**.
3. In the **Policy** pane on the right-hand side, scroll down to and right-click **Shutdown: Allow system to be shutdown without having to log on**.
4. Select **Properties**.
5. Click **Enabled** on the **Local Security Setting** tab, and then click **OK**.

CPU Element Resynchronization

Each system houses two CPU-I/O enclosures. Each CPU-I/O enclosure includes a CPU element and an I/O element. ftSMC represents these elements in the following nodes:

- **CPU Enclosure - 0** and **CPU Enclosure - 1**
- **I/O Enclosure - 10** and **I/O Enclosure - 11**

Discussions of CPU enclosures and I/O enclosures apply equally to the corresponding elements of CPU-I/O enclosures, unless otherwise specified.

A CPU element returning to service must resynchronize with the functioning CPU element. A CPU element requires resynchronization:

- After you bring down and then bring up a CPU element
- After a transient CPU element error
- After you power down a system and then power it up
- During online BIOS upgrade

During part of the resynchronization period, the system does not respond to network connections. Therefore, it is important to set the timeout period and/or number of retries for network applications to be large enough to prevent timeouts during resynchronization. The length of the resynchronization period is proportional to the amount of system memory configured.

By default, resynchronization occurs as soon as the CPU element that was taken out of service is determined to be operational or the failed enclosure is replaced. However, you can defer resynchronization to a more convenient time, such as an off-peak period.

See “Managing CPU Element Bringup” on page 2-4 for information about scheduling CPU bringup.

Managing CPU Element Bringup

You can specify two times of day at which to enable, or to which to defer, the return to service of CPU elements that have been removed from service (*shot*). You use two commands—Enable CpuBoard Bringup and Defer CpuBoard Bringup—which the Windows Scheduler executes. You also specify two times of day: one time when an offline CPU element can be brought up, and another time to which CPU Bringup is deferred. See ftSMC Help for instructions in setting these commands.

When Scheduler executes the commands, Enable CpuBoard Bringup changes the CpuBringUpPolicy property under the Srabid driver to **Enable Bringup**. This setting enables CPU elements that were removed from service to come back into service. It also brings up any CPUs that are in the Removed from Service state for a reason of Deferred BringUp, as long as they don't exceed the MTBF threshold.

When Scheduler executes the Defer CpuBoard Bringup command, it changes the CpuBringUpPolicy property under the Srabid driver to **Defer Bringup**. With this setting, if a CPU element is removed from service, the CPU elements come back into service at different times.

For example, consider the situation in which Defer CpuBoard Bringup is scheduled for every day at 8:00 a.m., and Enable CpuBoard Bringup is scheduled for every day at 9:00 p.m. In this case, if any CPU element gets removed from service after 8:00 a.m., it will not be allowed to come back into service until after 9:00 p.m., when Scheduler executes Enable CpuBoard Bringup. At that time, Enable CpuBoard Bringup will automatically bring up any CPU element that has been deferred between 8:00 a.m. and 9:00 p.m.

Controlling the Modem

CAUTION

When you replace or install a modem, turn off power to the modem connector to prevent damaging the modem and the system.

Use the following procedure to change the power state of the modem while the system remains online. Alternatively, shut down the system and remove the power cords, as described in the operation and maintenance guide for your system.

Powering the modem on or off while the system is online

1. In ftSMC, expand **ftServer (Local)** and **ftServer Call Home Modem**.
2. Refer to the PowerState property in the details pane, or the state of the power (green) LED on the modem, to verify that the power is on or off.
3. If the modem power is on, select **Initiate BringDown** to turn it off. If the modem power is off, select **Initiate BringUp** to turn it on.

Accessing Your System Desktop Remotely

You can remotely access your ftServer system's Windows desktop in different ways, depending on how your system is set up. Remote Desktop and VTM console enable remote access to the Windows desktop from a remote computer.

Enabling Remote Desktop

Microsoft Remote Desktop is installed by default on your system. However, it is not enabled by default.

NOTE

Users must have passwords to access remote desktops with the Remote Desktop application. See Microsoft documentation for details.

To enable Remote Desktop on a Windows Server 2003 system

1. Right-click **My Computer** and select **Properties**.
2. Click the **Remote** tab.
3. Select the check box under **Remote Desktop** to enable users to connect remotely to the computer.
4. The **Remote Sessions** dialog box will appear, stating that some local accounts might not have passwords. Click **OK**.

To enable Remote Desktop on a Windows Server 2008 system

1. Click the **Start** button.
2. Right-click **Computer** and select **Properties**.
3. In the list of Tasks, click **Remote settings**.
4. On the **System Properties** menu, click the **Remote** tab.
5. Under **Remote Desktop**, click **Allow connections from computers running any version of Remote Desktop (less secure)**.

Running ftSMC Remotely

See “Running ftSMC on a Remote System” on page 3-2 for details about running ftSMC on a remote system.

Booting or Shutting Down a System Through VTM Console

CAUTION

Before using the VTM console to turn off system power, always attempt to perform an orderly shutdown of the operating system.

You can use the VTM console to remotely access the server desktop to turn off system power and boot the host system. See “Using the VTM” on page 2-6 as well as the *Stratus ftServer Virtual Technician Module User’s Guide* (R642).

Using the VTM

To use the VTM, you must set up a VTM administrator account, and you must also log in to the VTM console. A VTM administrator account enables you to log in to the VTM Console. If necessary, you can assign a static IP address. See the *Stratus ftServer Virtual Technician Module User’s Guide* (R642) for related information.

Setting Up a VTM Administrator Account

You set up the account from ftSMC. (Note that the VTM administrator account is separate from your Windows administrator account.)

To set up a VTM administrator account

1. In ftSMC, expand **ftServer (Local)**, **ftServer Configuration**, right-click **ActiveService Network**, and select **Properties**.
2. On the dialog box, click the **SMM** tab.
3. Enter values into the following fields:
   - **SMM Admin ID**. Your VTM administrator login name.
   - **SMM Admin Password**. Your VTM administrator password.
4. Click **OK**.

Logging in to the VTM Console

To log in to the VTM console, you must first determine the IP addresses of the VTM network port of the baseboard management controllers (BMCs), then use the IP address of the port on the primary BMC in an Internet Explorer browser to access and log in to the VTM console.

To determine the IP address of the VTM network ports of the BMCs

1. In ftSMC, expand **ftServer (Local)**, **ftServer I/O Enclosures**, **I/O Enclosure - 10**, **BMC - 120**.
2. Note the IP address of the primary BMC from the ftSMC details pane.
3. Expand **I/O Enclosure - 11**, **BMC - 120**.
4. Note the IP address of the secondary BMC from the ftSMC details pane.

Copy these addresses in a location other than on the ftServer system, in case you need them to log in to the VTM console when the operating system is down or not responding.

To log in to the VTM console

1. Open an Internet Explorer browser, and enter the primary BMC IP address in the **Address** field.

   You can use an Internet Explorer browser on the ftServer system or on a remote system. For information on software and settings required on a remote system, see the *Stratus ftServer Virtual Technician Module User's Guide* (R642).

2. Log in to VTM using the login name and password that you entered when you set up the VTM administrator account.

Configuring Static IP Addresses for the VTM Network Ports

Typically, DHCP assigns IP addresses to the VTM network ports, which are at the rear of the system. However, if your environment requires static IP addresses, you can disable DHCP for the VTM network ports and then assign a different IP address to each of the ports.

To configure static IP addresses for the VTM network ports

1. In ftSMC, expand **ftServer (Local)**.
2. Expand **ftServer Configuration**.
3. Click and then right-click **VTM Network Config**, and click **Update Network Settings**.
4. In the **Enable DHCP** box, select **False**.

5. In the **Reserved VTM IP Address 1** box and the **Reserved VTM IP Address 2** box, enter two different IP address.
6. In the **Default Gateway for VTMs** box, enter the IP address of the default gateway.
7. In the **Subnet Mask for VTMs** box, enter a subnet mask.
8. Click **Finish**.

Using Windows System Event Logs

The system maintains logs of application, security, and system events. These event logs can help you or the CAC or your authorized Stratus service representative identify problems that have occurred on the system.

Windows Server 2003 and Windows Server 2008 include the following log files:

- **Application log**—The application log records events about system applications.
- **Security log**—The security log records events about system security.
- **System log**—The system log records events about general system activity.

Windows Server 2008 also includes:

- **Setup log**—The setup log contains events related to application setup.
- **ForwardedEvents log**—The ForwardedEvents log stores events collected from remote computers. See Windows online Help for more information about ForwardedEvents logs.

You can use **Event Viewer** to view the logs and to set the size of the application and system event logs. To prevent loss of event log data, maintain a regular schedule for manually saving event log files or obtain a third-party tool that saves event logs automatically.

Starting Computer Management

To start Computer Management

On a Windows Server 2003 or 2008 system, click **Start**, point to **Administrative Tools**, and then click **Computer Management**.

Setting the Size of Event Log Files

Specify the size of the event log files on your system.

CAUTION

Data will be overwritten if one of these event logs reaches its maximum log size.

To set the size of the application and system event logs in Windows Server 2003

1. Go to Computer Management, and click **Event View** to display its subnodes.

   Alternatively, click **Start**, **Administrative Tools**, and **Event Viewer**. Then click **Event View** to display its subnodes.

2. Click on the properties icon ( ).

   If **Event Viewer** does not display the properties icon ( ), click the subnode (for example, **Application**) of the log file whose size you want to set. Then, click **Properties**.

   In the **Log size** section, set the maximum log size in kilobytes (KB). The system default size for the application and system event logs is 2048 KB.

To set the size of the application and system event logs in Windows Server 2008

1. Go to Computer Management.
2. Expand **Event Viewer**, then **Windows Logs**.
3. Right-click the event log you want to manage (for example, **Application**) and select **Properties**.

   The other choices are Security, Setup, System, and Forwarded Events. (See Windows online Help for details about these event logs).

4. In the **Log Properties** dialog box, set the desired value in the **Maximum log size (KB)** box. The system default size for the application and system event logs is 2048 KB.
5. Click **OK**.

Saving Event Log Files

In the unlikely event that your system experiences problems, save the system event log and the application event log, in order to capture details relating to the problem.

Saving the log file has no effect on the current contents of the active log.

To save log files on a Windows Server 2003 system

1. Go to Computer Management, and click **Event View** to display its subnodes.

   Alternatively, click **Start**, **Administrative Tools**, and **Event Viewer**. Then click **Event View** to display its subnodes.

2. Right-click the subnode (for example, **Application**) of the event whose log file you want to save, and select **Save Log File As...** .
3. In the **Save *`Log File`* As** dialog box:
   - In the **Save In:** box, accept the default or enter a new path name.
   - In the **File name:** box, enter the file name.
   - In the **Save as type:** box, accept the default type, Event Log (*.evt). This allows you to view the saved file in Event Viewer.
4. Click **Save** to save the file.
5. After you save the log file, you can clear it. To clear the log, right-click the subnode, and then select **Clear all Events**.

To save log files on a Windows Server 2008 system

1. Go to Computer Management.
2. Expand **Event Viewer**, then **Windows Logs**.
3. Right-click the log you want to save, then click **Save Events As**.
4. In the **File name** box, enter a name for the saved file.
5. In the **Save as type** box, select a file format, then click **Save**.
6. Click **OK**.

See the Windows Server online Help for more options to the **Save Events As** command.

Monitoring ftServer Services

A number of ftServer services run on your system as Windows services. If any of these services is not running, the system does not function as designed. The *Stratus ftServer Systems: Technical Reference Guide* (R550) describes these services.

To check the status of a service:

1. Go to Computer Management.
2. Expand **Services and Applications**, and then click **Services**.

   Alternatively, click **Start**, **Administrative Tools**, and **Services**.

3. If a service's status is **Stopped** or blank, attempt to start the service by right-clicking it, and then clicking **Start**. If the service fails to start, check the event log for any messages related to the service.

Managing BIOS Settings

To manage BIOS settings, use the ftServer (BIOS) Setup utility.

To start the ftServer (BIOS) Setup utility

1. Turn on or reboot your system. The system begins booting with `Initializing Intel(R) Boot Agent GE v`*`n.n.nn`* messages.
2. Begin pressing **F2** to enter the ftServer (BIOS) Setup utility as soon as `Initializing..\` appears on the screen because initialization messages appear and disappear rapidly.

   Initialization messages include the following:

   ```
   Initializing Intel(R) Boot Agent GE vn.n.nn
   LSI Corporation MPT SAS BIOS
   Initializing..\
   Press Ctrl-C to start LSI Corp Configuration Utility...
   Searching for devices at HBA 0... followed by a list of two slots
   CPU = 2 Processors Detected, Cores per Processor = 4
   .
   [lines omitted]
   .
   Mouse initialized
   System Configuration Data updated
   SMBIOS Initialize..
   Press <F2> to enter SETUP or Press <F12> to boot from
   Network
   ```

   After you press **F2**, the message `Entering Setup` appears.

3. After executing some power-on self-test (POST) procedures, the system displays the Setup utility's **Main** menu. Use the RIGHT ARROW and LEFT ARROW keys to select different tabs. Use the UP ARROW and DOWN ARROW keys to select different settings on a page. Press the ESC key to return to a previous page. Press **Enter** to save new settings.

   NOTE

   On the **Security** tab, you can set a user or supervisor password. If a user or supervisor password is not set, the user or supervisor can enter Setup and modify any value. If a user or supervisor password is set, and a user or

supervisor enters Setup without the valid password, the user or supervisor can modify only the System Date and System Time, which are on the **Main** tab. If the user or supervisor enters setup with the valid password, then the user or supervisor can set or modify any value.

See the *Stratus ftServer Systems: Technical Reference Guide* (R550) for cautions and details about using the BIOS Setup utilities. See the *Stratus ftServer Virtual Technician Module User's Guide* (R642) for information on POST codes.

Determining the BIOS Version

Use ftSMC to determine the BIOS version. In ftSMC, click a **CPU Enclosure** node and look at the value of the BIOS: Stratus Version property in the details pane.

Writing to DVD-RWs on Windows Server 2003 Systems

Your ftServer system supports writing to DVD-RW drives. This capability is built into Windows Server 2008 systems. However, on Windows Server 2003 systems, you must enable the Image Mastering Applications Programming Interface (IMAPI), which is turned off by default, before writing to the DVD-RW drive.

To enable IMAPI

1. Right-click **My Computer** and click **Manage**.
2. Expand **Services and Applications** and click **Services**.
3. In the Services window, double-click **IMAPI CD-Burning COM Service**.

   The **IMAPI CD-Burning COM Service Properties** dialog box appears.
4. In the dialog box, under **Service Status: Stopped**, click the **Start** button.

   A message stating that Windows is attempting to start the IMAPI service appears. When the service is started, the **Service Status** value changes to **Started**.
5. On the General tab under Startup type, select **Automatic**.
6. Click **OK**.

Understanding Floppy Disk Drive Volume Letters

The operating system generally assigns the drive letter A to the optional floppy disk drive when the drive is first connected to a USB port. If you subsequently connect the drive to a different USB port or if the I/O element or element fails over, the operating system may assign the drive letter B to the floppy disk drive.

Using Serial Ports

Your system has two serial ports. Serial port 2 (Windows COM2) is always available for use by the operating system and is accessible to devices connected to its serial connector at the rear of the ftServer system. However, the availability of Serial port 1 (Windows COM1) is dependent on the presence or absence of an ASN modem in the ftServer system:

- If no ASN modem is installed in the ftServer system, Serial port 1 is also always available for use by the operating system and accessible to devices connected to **its** serial connector at the rear of the ftServer system.
- If the ASN modem **is** installed, Serial port 1 is normally dedicated to the ASN modem, is not available for general use by the operating system, and is not accessible to devices connected to its serial connector at the rear of the ftServer system.

You can determine the presence or absence of the ASN modem by examining the **ftServer Call Home Modem - 0** node in ftSMC, which will be shown as offline if no modem is present.

CAUTION

Although the serial ports have a nominal maximum speed of 115,200 bps, they do not operate reliably at speeds higher than 57,600 bps; so you should not attempt to run them at higher speeds.

Understanding Uninterruptible Power Supplies

Your ftServer system supports the use of an uninterruptible power supply (UPS) to power the system without interruption during short outages, and to gracefully shut the system down during longer power outages. As part of your fault-tolerant strategy, use a UPS qualified by Stratus.

- For information about qualified UPS models, see the site planning guide for your system.
- For UPS installation details, see the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).

If your ftServer system is not connected to a qualified UPS, the system may not have time to shut down gracefully in the event of a power failure, thus limiting your recovery procedure options. In that case, you have to reboot the system and verify that your file systems were not corrupted. Contact the Stratus CAC or your authorized Stratus service representative for further assistance.

Maintaining System Power During a UPS Failure

When you use a UPS qualified by Stratus, you connect that UPS to one half of the system. If a failure occurs in the UPS or in the UPS power source (for example, if the UPS is unplugged) and the backup battery runs low, the system continues to operate if the power to the non-UPS half of the system is unaffected by the failure.

Changing the IP Address of Systems with a UPS

If you change the IP address on the system, update the configuration on the UPS with the new IP address. If you do not update the UPS, and power to the system is automatically removed after a power failure, the system does not restart when power is restored.

NOTE

Assign a static IP address to the network interface that provides the connection to the UPS.

To change the IP address of systems with a UPS

1. In a Web browser, enter **http://** and the IP address of the UPS; for example, **http://*xxx.xxx.xxx***.
2. Log into the APC Web site using the user name and password.

   The IP address home page appears.
3. Click the **UPS** tab on the home page.
4. Click **clients** in the left-hand column beneath **Power Chute®**.
5. Click the IP address that you want to change.
6. In the **Client IP address box**, overwrite the existing IP address with the new IP address.
7. Click **Apply**.

Understanding SNMP Traps

Your ftServer system supports the Microsoft SNMP Agent, which enables third-party Enterprise Management consoles to remotely monitor the systems. The ftServer SNMP Agent provides a standard mechanism for monitoring the status of systems and for receiving alarms from the systems.

During instances of system malfunction or in response to a system event, such as a firmware update, you may see multiple traps in third-party management consoles for various devices. For instance, if a PCI adapter fails, the SNMP agent may send traps not only for the adapter but also for its slot. You may safely disregard these traps.

See the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) for SNMP configuration information.

Understanding Updates and Hotfixes

See the following Web page for an up-to-date statement of Stratus' policy on installing upgrades and hotfixes to the operating system:

http://www.stratus.com/support/releasepolicy

You can greatly reduce application downtime when you upgrade software by installing and using the optional Stratus ftServer Active Upgrade software. If you do plan to install and use Active Upgrade software, be sure to keep system files on a separate disk from data files. See the *Stratus ftServer: Active Upgrade User's Guide* (R017W) for more information.

Avoiding Problems

To take full advantage of your system's fault-tolerant features and to avoid problems, observe the following when setting up and operating your system:

- **Do not attempt to boot the system from a network drive.** Booting the system from a network drive is not supported**.**
- **Do not use Windows Device Manager to disable devices except in documented special situations.** Using Windows Device Manager to disable devices can interfere with the proper operation of your system. The correct way to take devices out of service and return them to service is through the ftSMC snap-in. However, to handle special situations, the system documentation may instruct you to use Windows Device Manager.
- **Do not turn on the Emulex elxstor.sys LightPulse Storport Miniport driver services; they will interfere with the fault-tolerant operation of your system.** Upon installation, these services are set to manual.
- **Do not install devices unless they have been tested and certified as compatible with ftServer systems.** Installing devices that have not been tested and certified to be compatible with your ftServer system can reduce the fault tolerance of your system. If you want to install a device that has not been certified, contact your account team.

Chapter 3
ftSys Management Console

ftSys Management Console (ftSMC) is described in the following major sections:

- "ftSMC Overview" on page 3-1
- "Running ftSMC" on page 3-2
- "Performing ftSMC Tasks" on page 3-6
- "CPU and I/O Enclosures and Elements" on page 3-12

For information about the Virtual Technician Module (VTM), see the *Stratus ftServer Virtual Technician Module User's Guide* (R642) and ftSMC Help.

ftSMC Overview

ftSMC, an MMC snap-in, is the system management tool you use to monitor and control the operation of your system. ftSMC presents a list of the system components in the console tree and properties of the component in the details pane.

For example, to determine which model ftServer you have, perform the following steps:

1. On the Windows Desktop, click the **ftSys Management Tools** icon.
2. Expand **ftServer (Local)**, **ftServer Drivers**, and **System ID PROM - SystemIdProm**.

   In the Details pane, the ModelDesc and ModelName properties identify the system model and P-package, respectively. The ModelDesc property presents a simple model-name value, like ftServer 4500. The ModelName property presents one of the values explained in Table 3-1.

Table 3-1. ftServer System Models by P-Package

ModelName Value	System Model
P2600-1S	ftServer 2600 rack-mountable dual-core 1-way
P4500-1S	ftServer 4500 rack-mountable quad-core 1-way
P4500-2S	ftServer 4500 rack-mountable quad-core 2-way
P6300-2S	ftServer 6300 rack-mountable quad-core 2-way

Use ftSMC to disable devices. Do not use Windows Device Manager to disable devices except in documented special situations.

NOTE

MMC snap-ins, including ftSMC, do not lock edit sessions to prevent simultaneous users from editing the same parameters.

Running ftSMC

You can run ftSMC the following ways:

- Directly on your ftServer system
- On a remote computer
- From a remote computer by accessing your ftServer system desktop remotely

Running ftSMC Directly on Your ftServer System

You can run ftSMC directly on your system in two ways.

To run ftSMC from the desktop of an ftServer system

Click the **ftSys Management Tools** shortcut on your system's desktop.

To run ftSMC by navigating to its executable file

1. From the desktop, double-click the **Computer** icon (on systems running Windows Server 2008) or the **My Computer** icon (on systems running Windows Server 2003).
2. Double-click **Local disk (C:)**, **Program Files**, **ftSys**, and then **management**.
3. Double-click **ftServer**.

Running ftSMC on a Remote System

You can run ftSMC on a remote system by adding the ftSMC snap-in to a remote system that is running Windows 2000, Windows Server 2003, Windows XP, Windows Vista, or Windows Server 2008:

1. Install ftSMC on a supported computer, using the Remote Management Installation (RMI) procedure described in the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).
2. Add the ftSMC snap-in to MMC, specifying an ftServer system to manage and saving the console that contains the snap-in.

After you have added a console, you can open a previously saved MMC console that contains ftSMC.

(Instead of, or in addition to, adding the ftSMC snap-in, you can access the ftServer system's desktop remotely, in order to run ftSMC from a remote system. For information, see "Accessing Your System Desktop Remotely" on page 2-5.)

Adding the ftSMC Snap-in to MMC on a Windows Server system

To add the ftSMC snap-in to MMC on a Windows system, you must:

1. Modify security on the remote system using the DCOM configuration utility (dcomcnfg.exe).
2. Modify the Windows Firewall and Advanced Security settings on the ftServer system.
3. Add the ftSMC snap-in on the remote system.

Modifying security on the remote system using dcomcnfg.exe

CAUTION

Modifying security on the remote system using the DCOM configuration utility can compromise the security of the system.

1. From the **Start** menu of the remote computer, click **Run**, type **dcomcnfg** in the **Open** box, and click **OK**.
2. In the **Component Services** window, expand **Component Services**, **Computers**, and then **My Computer**.
3. Right-click the **My Computer** icon and select **Properties**.
4. Select the **COM Security** tab.
5. Under **Access Permissions**, select **Edit Limits**.
6. Select **ANONYMOUS LOGIN** from the **Group or user names** box, and then check the **Allow** box for **Remote Access**.
7. Click **OK** in the **Access Permissions** window.
8. Click **OK** in the **My Computer** window.
9. Close the **Component Services** window.
10. Reboot the system.

Continue by modifying the Windows Firewall and Advanced Security settings on the ftServer system.

Modifying the Windows Firewall and Advanced Security settings on the ftServer system

CAUTION

Modifying Windows Firewall and Advanced Security settings on the ftServer system can compromise the security of the system.

1. Access **Windows Firewall and Advanced Security** on the ftServer system (for example, click **Start**, **Administrative Tools**, and then **Windows Firewall and Advanced Security**).
2. Click **Inbound Rules**.
3. Find and then enable the following rules:
   - Remote Administration (NP-In)
   - Remote Administration (RPC)
   - Remote Administration (RPC EPMAP)

Continue by adding the ftSMC snap-in.

Adding the ftSMC Snap-in on the remote system

1. From the **Start** menu of the remote computer, click **Run**, type **mmc** in the **Open** box, and click **OK**.
2. In the **Console1** window of MMC, click the **File** menu item, and click **Add/Remove Snap-in**.
3. In the **Add/Remove Snap-in** dialog box, click **Add**.

   The **Add Standalone Snap-in** dialog box appears with a list of snap-ins.
4. Click **ftServer Management Console** and click **Add**.

   The **Connect** dialog box appears.
5. Type the *servername.domainname* or the IP address of the server (for example, usbos01.wtcus.com or 192.168.57.10), and select or clear the **Connect as current user** check box. If you clear the check box, type the user name and password that will be used to make the connection.

   NOTES

   1. The user name that you enter must be in the Windows Administrators group for the computer that you want to manage.

2. You can select any remote ftServer system to manage, as long as you have appropriate access to it.

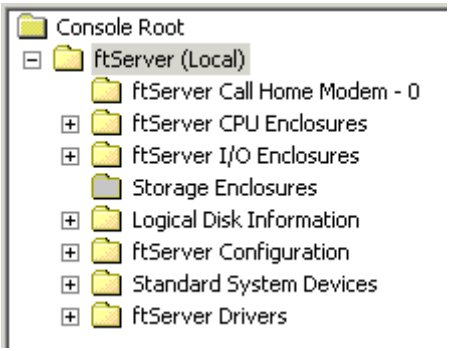
6. Click **Close** in the **Add Standalone Snap-in** dialog box.
7. Click **OK** in the **Add/Remove Snap-in** dialog box.

   The name of the system appears in MMC. The ftSMC snap-in displays information about the system and you can use the ftSMC snap-in to manage the system.

8. Save this console, with ftSMC added, for later use by clicking **Save As** in the **Console** menu. In the **Save As** dialog box, type a file name in the **File Name** box, and click **Save**.

Figure 3-1 shows an example of an ftSMC snap-in tree on a remote management computer. The ftServer system being managed includes an optional **ftServer Call Home Modem**, but no optional attached storage enclosures (the Storage Enclosures node is blank).

Figure 3-1. ftSMC Tree



Opening a Previously Saved MMC Console

1. Click **Start**, and then click **Run**.
2. In the **Run** window, type **mmc** in the **Open** box, and then click **OK**.
3. In the **Console** window, click the **File** menu, then **Open**.
4. In the **Open** window, double-click the name of the previously saved MMC console.

Performing ftSMC Tasks

Detailed instructions for using ftSMC are available in ftSMC Help. Before interacting with ftSMC, note the following cautions.

CAUTION

Before using ftSMC to interact with the Stratus Customer Assistance Center (CAC) or your authorized Stratus service representative, perform the tasks described in the *Stratus ActiveService Network Configuration Guide* (R072).

CAUTION

When working in ftSMC, generally do not change the configured values of properties unless directed to do so in documentation or by the CAC or your authorized Stratus service representative.

When you click a command that does not have an ellipsis, the system performs the command immediately and a dialog box displays the status of the command, for instance, **The operation completed successfully**. This status does not indicate that the selected procedure has completed, but only that the command has been successfully initiated. Click **OK** in the dialog box to dismiss it. Monitor the state of the device in the details pane or the system event log to see if the command completed successfully.

ftSMC Interface

The details pane, the icons used in ftSMC, and the ftSMC display refresh options are features of the ftSMC interface. Figure 3-2 shows the ftSMC user interface.

To expand all nodes, press the asterisk (*) key on the number pad.

NOTE

In ftSSS for the Windows Operating System, Release 6.0.0, ftSMC provides functionality under the **BMC - *n*** node that ftSMC of previous ftSSS releases provided under the **VTM adapter - *n*** node.

Figure 3-2. ftSMC User Interface

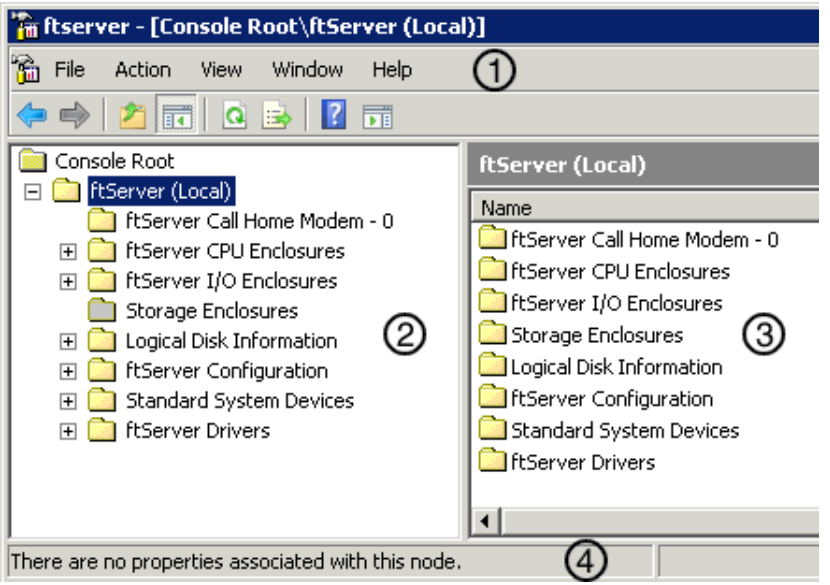


Table 3-2 describes the key elements in the ftSMC user interface.

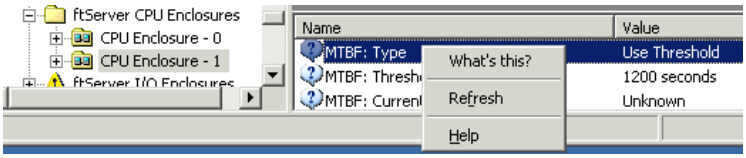
Table 3-2. ftSMC User Interface Key Elements

Item	Description	Function
1	Action band	The Action menu contains MMC snap-in commands. The View menu contains console viewing options.
2	Console tree	Lists all system component nodes. Each node represents a manageable object.
3	Details pane	Displays the properties related to the node selected in the console tree. For an explanation of a property, right-click the property and select **What's this?** from the shortcut menu to display information from ftSMC Help. (Not all properties have What's this? help.) The *Stratus ftServer Systems: Technical Reference Guide* (R550) includes information about properties.
4	Status bar	Displays ftSMC status messages.

Details Pane

The names and values of the properties of the components in the ftSMC tree are displayed in the details pane. A question mark (**?**) icon in front of a property name indicates that What's this? Help is available in ftSMC Help. Right-click the property name and click in the shortcut menu that appears. See Figure 3-3.

Figure 3-3. Using What's This? in the Details Pane



Icons Used in ftSMC

Figure 3-4 shows the icons used in the system inventory.

Figure 3-4. System Inventory Icons

- A dimmed folder icon indicates that the node does not contain any information. It is **empty**.
- A plain, yellow folder icon indicates that the node is **online** and contains information or child nodes. This icon indicates online simplex components.
- A tools icon indicates that the node is **offline**, possibly for maintenance.
- A dual-monitor icon indicates that the node is **duplexed** (partnered) with another node (for example, two CPU elements).

  NOTE

  It is safe to remove a duplexed component.

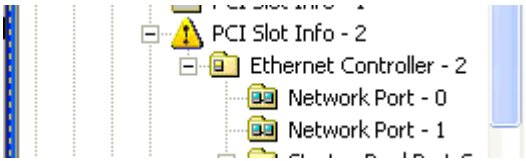
- A magnifying glass icon indicates that the node is offline and undergoing diagnostic **testing**.
- A single-monitor icon indicates that the component is operating **simplexed** (unpartnered).

NOTE

It is unsafe to remove a simplexed component from the system. Removing a simplexed component causes loss of that component function to the system.

The simplexed icon can also indicate an invalid configuration. For instance, the simplexed icon next to Ethernet Controller - 2, shown in Figure 3-5, indicates that Network Port - 0 and Network Port - 1 beneath the Ethernet Controller - 2 are duplexed, but that Ethernet Controller - 2 is simplexed, which makes it a single point of failure, an illegal configuration.

Figure 3-5. Simplexed Icon for Invalid Configuration



ftSMC displays warning and error icons described in Table 3-3.

Table 3-3. ftSMC Warning and Error Icons

Icon Type	Description	Indication
Warning	Exclamation point inside a yellow triangle	A node whose child node has an error.
Error	White X inside a red circle	The node is offline, in testing, or has failed.
No inventory found	White X inside a gray circle	ftSMC cannot retrieve inventory information for that device. The ftSMC status bar displays a message indicating that the properties cannot be retrieved.
Threshold warning	Exclamation point inside a red triangle	The current reading of a sensor value exceeds the specified threshold. Parent nodes display the yellow warning icon.

Figure 3-6 shows an error icon next to **Network Port - 1**, indicating an error on that node. Warning icons precede the names of all parent nodes that have nodes with an error.

Figure 3-6. Warning and Error Icons

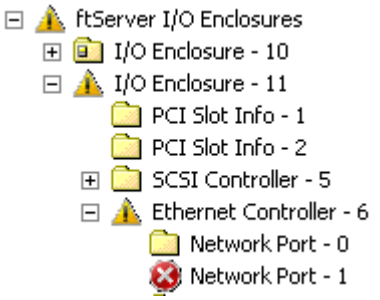

ftServer I/O Enclosures
I/O Enclosure - 10
I/O Enclosure - 11
PCI Slot Info - 1
PCI Slot Info - 2
SCSI Controller - 5
Ethernet Controller - 6
Network Port - 0
Network Port - 1

Figure 3-7 shows a no-inventory-found icon next to the CPU Enclosure icons.

Figure 3-7. Warning and Inventory Error Icons

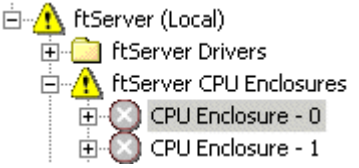


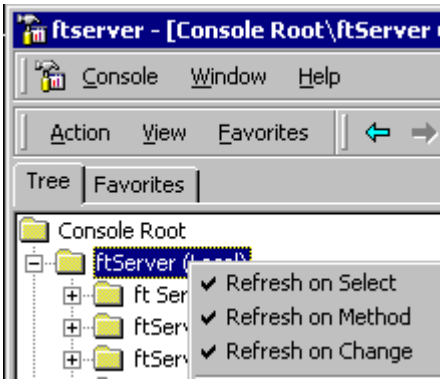
Figure 3-8 shows a threshold warning icon for a voltage sensor.

Figure 3-8. Threshold Warning Icon

Refreshing the ftSMC Display

You can right-click the ftServer (Local) root node to enable or disable each of three refresh options. These options cause ftSMC to refresh, or update, the information in the details pane when the specified event occurs. You should enable these options so that the details pane and the node icons update when you complete an action or when a state change occurs. When enabled, a check mark appears in front of the option, as shown in Figure 3-9.

Figure 3-9. ftSMC Details Pane Refresh Options



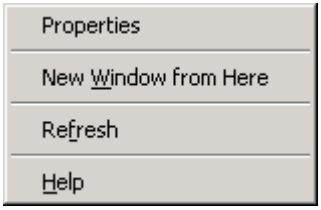
Viewing and Changing Properties

To view the properties of a system inventory component, click the component's node in the console tree. The names and values of that component's properties are displayed in the details pane, as shown in Figure 3-3.

Some components' properties are configurable. Components with configurable properties have a **Properties** command in their shortcut menu. See Figure 3-10.

See ftSMC Help for details.

Figure 3-10. Properties Command in Shortcut Menu



Required Operational States for Commands

Table 3-4 presents the operational state that a device must be in to carry out the associated command.

Table 3-4. Operational State for Associated Commands

Command	Valid States
CPU Element	
Initiate BringUp	Removed, Broken, Shot, Firmware update complete, Diagnostics passed.
Initiate BringDown	Broken, Firmware update complete, Diagnostics passed, Duplex.
Initiate Diagnostics	Removed, Broken, Firmware update complete, Diagnostics passed.
Set Priority	CPU element must be online and duplexed.
I/O Element	
Initiate BringUp	Removed, Broken, Shot, Diagnostics passed.
Initiate BringDown	Broken, Diagnostics passed, Duplex.
Initiate Diagnostics	Removed, Broken, Diagnostics passed.

CPU and I/O Enclosures and Elements

Each system houses two CPU-I/O enclosures. Each CPU-I/O enclosure contains a *CPU element* and an *I/O element* joined to the same board. You can monitor each CPU element and I/O element separately. ftSMC represents these elements in the following nodes:

- CPU Enclosure - 0 and CPU Enclosure - 1
- I/O Enclosure - 10 and I/O Enclosure - 11

Descriptions of CPU elements and I/O elements apply to the elements of both CPU-I/O enclosures, unless otherwise specified.

Primary and Secondary CPU-I/O Enclosures

Both CPU-I/O enclosures in an ftServer system process every instruction in lockstep, but only one CPU-I/O enclosure is the *primary*, or *active*, enclosure at a time. The other CPU-I/O enclosure is the *secondary* enclosure; it assumes the role of primary enclosure only if the previously primary enclosure fails or is taken out of service. But,

under certain circumstances, you can force the secondary enclosure to become the primary enclosure.

For example, your authorized Stratus service provider might ask you to switch the primary enclosure for troubleshooting purposes. Or, if you are about to run the Active Upgrade process, you might want the enclosure that is connected to UPS-protected power (CPU enclosure 0, I/O enclosure 10) to be the primary enclosure, because this provides better protection for your system if power fails during the upgrade (especially while your system is in *split mode*).

Switching the Primary CPU-I/O Enclosure

If you need a particular CPU-I/O enclosure to be primary, first check the operational state of that enclosure. If it is currently the secondary enclosure, you can manually set that enclosure to become the primary enclosure.

To check the operational state of an I/O enclosure

1. Open ftSMC.
2. Expand **ftServer (Local)**.
3. Expand **ftServer I/O Enclosures**.
4. Click **I/O Enclosure - *n***. (To prepare for the Active Upgrade process, check the state of **I/O Enclosure - 10**.)
5. Verify that the value for **Op State: Reason** is **Primary** and the value for **ActiveCompatibilityFlag** is **True**.

If the value for **Op State: Reason** is **Secondary** and the value for **ActiveCompatibilityFlag** is **False**, you can manually set the enclosure to be the primary enclosure.

To make an I/O enclosure the primary I/O enclosure

1. Open ftSMC.
2. Expand **ftServer (Local)**.
3. Expand **ftServer I/O Enclosures**.
4. Expand **I/O Enclosure - *n***. (To prepare for the Active Upgrade process, expand **I/O Enclosure - 10**)
5. Right-click on the I/O enclosure.
6. Click **Make Active Compatible**.

If you are preparing for the Active Upgrade process, you might need to wait 5-10 minutes for the system components to stabilize and return to full duplex mode before running a readiness check.

Chapter 4
Disk Storage Management

The following disk-management topics apply to your ftServer system:

- "Data Fault Tolerance" on page 4-1
- "Guidelines for System Disks" on page 4-2
- "Using RDR for Mirroring and Fault Tolerance" on page 4-2
- "Managing RDR Disks" on page 4-4
- "Using Volume Mirroring for Fault Tolerance" on page 4-25
- "Using Hardware RAID Controllers For Fault Tolerance" on page 4-27
- "ftSMC Interface for Storage Enclosures and Subsystems" on page 4-27
- "Mirroring Disks in ftScalable Storage Systems" on page 4-29
- "Finding an Internal Physical Disk" on page 4-29
- "Finding an External Physical Disk" on page 4-31

Data Fault Tolerance

Your ftServer system offers these methods of ensuring data fault tolerance and continuous availability of its disk media:

- Rapid Disk Resync (RDR), a disk-replicating technology, is supported on the internal disk drives.
- On optional ftScalable Storage systems, you use the RAIDar graphical user interface to create virtual disks in the external storage. See the *ftScalable Storage: Getting Started Guide* (R601) for details.

  After creating the virtual disks using RAIDar, you must use Windows Disk Management or another disk-management tool to initialize the virtual disks and format the volumes on them.
- If you are not using RDR or RAIDar, see your disk-management tool documentation for information on how to create striped volumes across the mirrored internal disks.

NOTE

Create a backup of the system disk with which to restart the system in the unlikely event of a system failure. See the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).

Guidelines for System Disks

On the system disk, the IPL procedure creates a boot partition, which contains the operating system and all of its components.

Because the system disk and boot partition hold system-critical files, such as the paging file and system event files, limit the traffic to this disk to system traffic only.

The internal storage of your ftServer system supports Serial Attached SCSI (SAS). The system's disks are located in a disk tray that connects to the system backplane.

NOTE

You may use any slots for any disks, with the following two exceptions. First, pair disks in partner I/O elements, not within the same element, to promote fault-tolerance. Second, use a SAS disk for the system boot disk and locate it in the bottom-most slot (Slot-1).

You can greatly reduce application downtime when you upgrade software by installing and using the optional Stratus ftServer Active Upgrade software. If you plan to install and use Active Upgrade software, be sure to keep system files on a separate disk from data files. See the *Stratus ftServer: Active Upgrade User's Guide* (R017W) for more information.

Using RDR for Mirroring and Fault Tolerance

Use RDR disk mirroring to configure and create managed disks in internal storage. With RDR disk mirroring, you mirror pairs of physical disks to create *RDR virtual disks*. Each pair of mirrored disks constitutes one RDR virtual disk. RDR offers faster resynchronization of mirrored disks than other mirroring methods after transient failures or when a single disk is briefly removed from service.

NOTE

In RDR terminology, an individual physical disk is also called a *plex*, and an RDR virtual disk is also called a *LUN*, for *logical unit*.

The data on one disk of the RDR virtual disk pair is replicated in full—that is, *mirrored* or *duplex*—on its corresponding partner disk, irrespective of volume or partition layout.

However, an RDR virtual disk may also be *simplex* (consisting of only one physical disk). A simplex RDR virtual disk may contain mirrored volumes created using third-party disk management facilities. If all volumes on a simplex RDR disk are mirrored with other disks in the system, then the simplex RDR disk is effectively duplex (mirrored).

If you are upgrading a system's disks from a non-RDR to an RDR configuration, the existing disks must provide adequate space for metadata. *Metadata* is "data about data" that the RDR software stores on disks to implement disk management. When you configure a disk for RDR, the system displays an error message if the disk does not have adequate space. The disk being upgraded should be a basic disk. A *basic disk* is one that is divided into partitions.

RDR virtual disks appear in ftSMC under the Logical Disk Information node. In this location, the details pane presents the location of the physical disks in the RDR virtual disk in these properties:

- Disk Enclosure Slot: DevicePath[2]
- Disk Enclosure Slot: DevicePath[1]

However, the DevicePathID property that appears at the top of the details pane, and which has a number like 39/7, does not indicate a hardware component and does not signify the physical disks's location in the system; it merely identifies the virtual disk to system-management software.

See Table 4-1 for the RDR disk numbering scheme.

Automatic Virtual Disk Expansion

An RDR virtual disk includes an automatic disk-capacity expansion feature. If you replace the physical disks (plexes) of an RDR virtual disk with larger physical disks, RDR automatically recognizes the resulting larger virtual disk, which enables the system to use the added disk capacity.

Note, however, that a virtual disk cannot be larger than the smaller of its two physical disks. For example, if each physical disk of an RDR virtual disk is 80 gigabytes (GB), the virtual disk is an 80-GB virtual disk. If you replace one 80-GB physical disk with a

160-GB physical disk, the virtual disk remains an 80-GB disk, the smaller of the two physical disks. But if you replace the other 80-GB physical disk with another 160-GB physical disk, the RDR virtual disk automatically updates to 160 GB.

ftSMC reports the capacity of physical disks and virtual disks in the Capacity property in two different locations:

- The physical disk Capacity property appears in the ftSMC details pane under **ftServer I/O Enclosure - 10**, **Storage Enclosure - 40**, **Slot - *n***, **Disk - *n***.
- The virtual disk Capacity property appears in the ftSMC details pane under **Logical Disk Information**, **RDR Virtual Disk - *n***.

Automatic virtual disk expansion does not work on *dynamic virtual disks*—that is, RDR virtual disks that have been converted to dynamic disks by Windows Disk Management. (A *dynamic disk* consists of a single partition that is divided into volumes. Dynamic disks can be combined with other disks to form volumes that expand beyond a single disk.)

Managing RDR Disks

Managing RDR-configured disks can include any of the following tasks:

- Configuring the first plex of an RDR virtual disk
- Using RDR to mirror disks
- Enabling write caching and read-load balancing
- Setting the active RDR disk (plex)
- Deleting RDR configuration on a physical disk
- Removing a physical disk from and RDR virtual disk
- Deporting a physical disk from an RDR virtual disk
- Creating a Spare Bootable RDR Disk
- Breaking a Physical Disk from an RDR Virtual Disk
- Converting disks from dynamic to basic
- Setting or clearing the mean-time between failure (MTBF) threshold
- Resynchronizing a physical disk from the RDR virtual disk
- Setting the MTBF faultcount limit
- Making a backup of a boot disk
- Booting with a backup disk
- Reusing dynamic disks
- Recovering a disk

- Verifying disk integrity
- Avoiding a Stale-Disk Boot
- Prioritizing resynchronization

To use RDR to mirror dynamic disks, see the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).

You can also set disk parameters from the **SCSI Port Duplex Driver - Sradisk_Driver** node shortcut menu in the ftSMC.

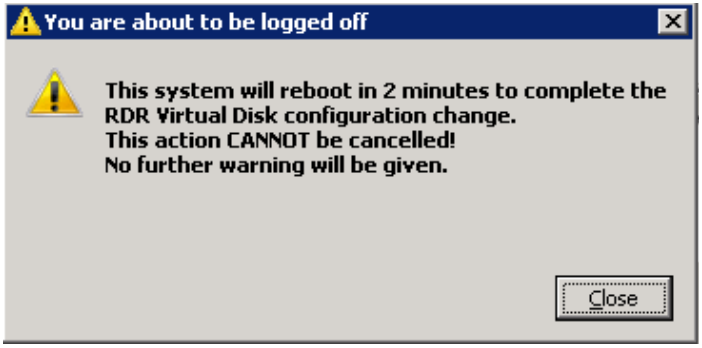
Creating a First RDR Virtual Disk

To create an RDR virtual disk, you use the **Create RDR Virtual Disk** action from the context menu of a disk. Then you add a physical disk to the RDR virtual disk on another physical disk to make the two physical disks into a single RDR virtual disk.

If you create the first RDR disk (plex) on a disk that already has data on it (for instance, a system disk), make sure that both disks have the same capacity, that the disks are basic disks (not dynamic), and that the second disk (the one to be the mirror) has no partitions.

To configure the first plex of an RDR virtual disk

1. In ftSMC, expand **ftServer (Local)**, **ftServer I/O Enclosures**, **I/O Enclosure - 10** (or **11**), **Storage Enclosure - 40**, **Slot - *n***, and then right-click **Disk - *n***.
2. Click **Create RDR Virtual Disk**.
3. At the message about a possible system reboot, click **Yes**.
   a. On a Windows Server 2008 system, you will see the following message.


You are about to be logged off
This system will reboot in 2 minutes to complete the RDR Virtual Disk configuration change.
This action CANNOT be cancelled!
No further warning will be given.
Close

The system automatically reboots.

b. On a Windows Server 2003 system, click **OK** on the dialog box that indicates that the command was successfully requested.

   If necessary, follow the prompts to reboot the system.

Mirroring Disks Using RDR

The procedure used to mirror disks with RDR is the same used to upgrade a disk to RDR. To mirror an RDR disk, you give the Add Physical Disk To RDR Virtual Disk command on an unconfigured disk (the target) and overwrite it with an existing RDR-configured disk (the source).

If you are upgrading disks to use RDR, be sure that the disks are basic disks. (*Basic disks* are divided into partitions. *Dynamic disks* consist of a single partition that is divided into volumes. Dynamic disks can be combined with other disks to form volumes that expand beyond a single disk.) If the disks have been configured as dynamic disks, convert the disks to basic disks before upgrading them to RDR (refer to Windows online help).

Although you can only create RDR disks from basic disks, you can make RDR disks dynamic if your policies require it.

If you insert a blank (having no disk signature or volume ID), non-RDR-configured disk into a slot previously occupied by an RDR disk whose partner slot is currently occupied by an RDR disk, the system automatically adds the inserted disk to the RDR virtual disk.

Not all RDR commands and procedures are valid on all physical disks. Error messages appear if you attempt an invalid RDR command. Error messages also suggest possible corrective actions, where applicable.

Some RDR configuration changes, especially those made on simplex RDR virtual disks, may require the operating system to restart in order to complete. When the Windows restart warning appears, you can restart the system immediately or defer restarting until a more convenient time.

RDR Disk Numbering

Internal storage disks and RDR virtual disks are labeled with numerical IDs that appear in ftSMC. See Table 4-1 for the locations of the Disk and RDR Virtual Disk nodes.

NOTE

In Table 4-1, the *n* designates a variable number. The numbers vary because the operating system assigns

them dynamically as individual disks and RDR virtual disks are removed from and returned to the system.

Table 4-1. RDR Disk Numbering

ftServer (Local)\ftServer I/O Enclosures\I/O Enclosure - *n*\ Storage Enclosure - 40	**ftServer (Local)\Logical Disk Information**	**Location in Internal Storage Enclosure**
Slot-1, Disk-*n*	RDR Virtual Disk *n*	**Bottom** drive
Slot-2, Disk-*n*	RDR Virtual Disk *n*	Middle drive
Slot-3, Disk-*n*	RDR Virtual Disk *n*	**Top** drive

Adding a Physical Disk to an RDR Virtual Disk

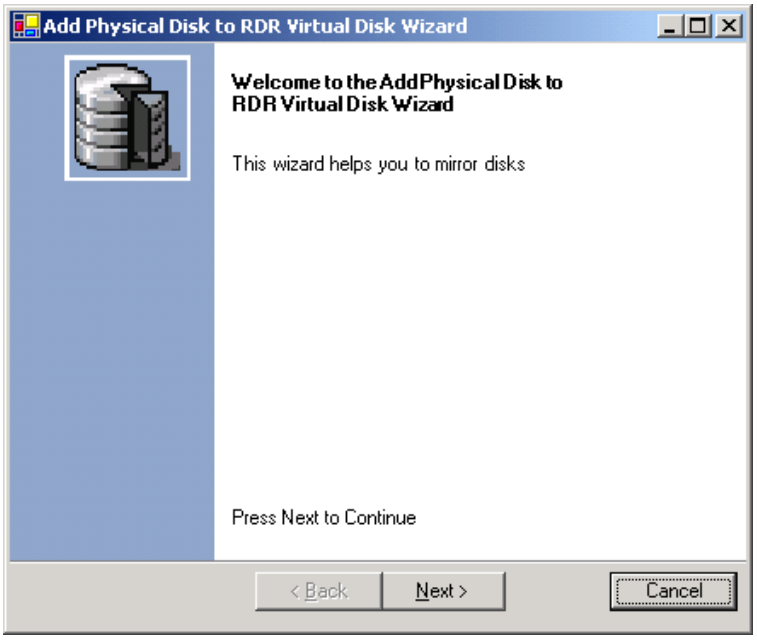
To add a physical disk to an RDR virtual disk, perform these steps.

1. In ftSMC, expand **I/O Enclosure**, **Storage Enclosure - 40** and **Slot - *n***, and then select the disk (the *target* disk) that you want to add to the RDR virtual disk.

   The target disk must be an unconfigured (nonRDR-configured) disk.

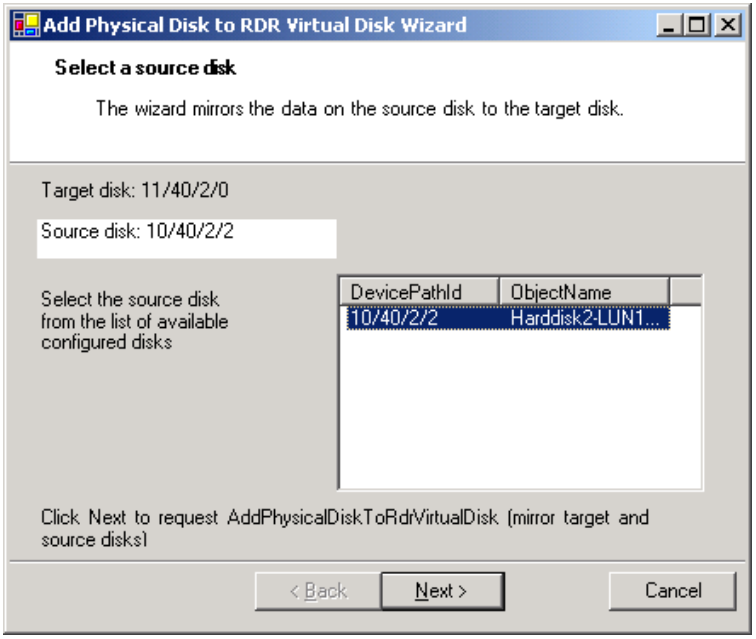
2. Right-click the target disk and select **Add Physical Disk to RDR Virtual Disk**.

   The following disk wizard appears.


Add Physical Disk to RDR Virtual Disk Wizard
Welcome to the Add Physical Disk to RDR Virtual Disk Wizard
This wizard helps you to mirror disks
Press Next to Continue
< Back
Next >
Cancel

3. Click **Next**.

   The **Select a source disk** dialog box appears, identifying the target disk and the disk or disks available for being chosen as sources.


Add Physical Disk to RDR Virtual Disk Wizard
Select a source disk
The wizard mirrors the data on the source disk to the target disk.
Target disk: 11/40/2/0
Source disk: 10/40/2/2
Select the source disk from the list of available configured disks
DevicePathId
ObjectName
10/40/2/2
Harddisk2-LUN1...
Click Next to request AddPhysicalDiskToRdrVirtualDisk (mirror target and source disks)
< Back
Next >
Cancel

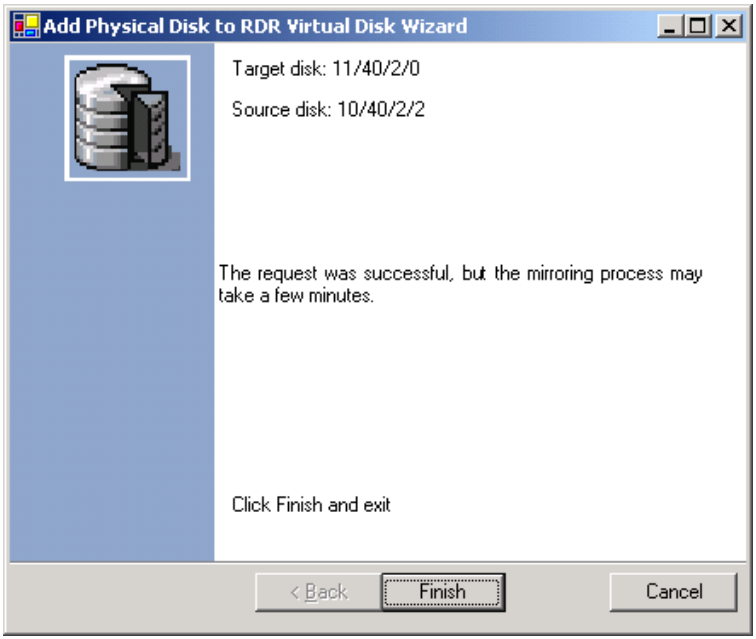
   A source disk will already be selected by default in the **Select a source disk** dialog box, if storage-enclosure rules allow.

4. If a source disk is not already selected in the dialog box, choose a source from the available disks listed in the right-hand box within the dialog box, and click **Next**.

   The RDR virtual source disk will overwrite the unconfigured target disk, making it a mirror of the RDR virtual source disk.

   In this example, only one source disk, the disk in 10/40/2/2, is available.

   The following screen appears, identifying the source and target disks.


Add Physical Disk to RDR Virtual Disk Wizard
Target disk: 11/40/2/0
Source disk: 10/40/2/2
The request was successful, but the mirroring process may take a few minutes.
Click Finish and exit
< Back
Finish
Cancel

5. Click **Finish**.

   The system mirrors the source disk to the target disk. The mirroring process may take a half-hour or more, depending on the size of the disks.

   While the disks are resynchronizing, LEDs blink to indicate read and write operations, and ftSMC displays a value of OpState: State Syncing in the details pane for the disk.

   To view the progress of the synchronization in ftSMC, expand **Logical Disk Information** under **ftServer**, and select the virtual disk. In the details pane, the progress is noted as a percentage, as follows:

   ```
   Status: Resync: 20 percent
   ```

   When the disks are synchronized, the LEDs on both disks are lit steady green and ftSMC displays a value of OpState: State: Duplex in the details pane for the disk and for the virtual disk. The value next to Status for the virtual disk is None.

   NOTE

   If you receive an error message when using the **Add Physical Disk To RDR Virtual Disk** command, the disk you are trying to add may not have sufficient free space for

the metadata. Be sure the disk has a minimum of 10MB free space.

A **System Shutdown** message may appear, stating that the system will reboot in two minutes. If the message appears, let the system restart.

NOTES

1. If you added a system disk to an RDR virtual disk, a message notifies you that the system will reboot. The message gives you the option of confirming or cancelling the request.
2. The system restarts if you add a data disk to an RDR virtual disk and the software cannot unmount all data volumes on the disk.
3. You cannot add a physical disk to RDR if the disk is dynamic or a nonblank data disk.

Disk Failures During Resynchronization

In RDR resynchronization, partnered RDR virtual disks relate as *source* and *target* disks. The source is the disk from which the target disk is being resynchronized.

If a source disk fails or is removed from service during resynchronization, the target disk is removed from the system and treated as a deported disk. If the target disk fails or is removed from service during resynchronization, the source disk continues operating in simplex mode.

If the system starts to shut down while an RDR virtual disk is resynchronizing, RDR records the state of the resynchronization and, upon system reboot, resumes resynchronization from that point.

Write Caching

To optimize system performance, you can enable write caching on RDR virtual disks. By default, write caching is disabled, except during disk resynchronization, when it is automatically enabled.

Write caching does not work on a simplex RDR virtual disk (except when it is resynchronizing), even if it is enabled. However, if you enable write caching on a simplex disk that is later duplexed, write caching will work.

To enable write caching

1. Go to Computer Management.
2. Click **Device Manager**, and then expand **Disk Drives** in the right-hand panel.

3. Right-click the target disk, select **Properties**, and click the **Policies** tab.
4. Check **Enable write caching on the disk**, and click **OK**.

Setting the Cache Flush Interval

The **Set Cache Flush Interval** command determines the interval at which the system deletes the unaccessed contents of the cache buffer on an RDR virtual disk.

To set the cache flush interval

1. In ftSMC, expand **ftServer (Local)** and click **Logical Disk Information**.
2. Right-click the desired RDR Virtual Disk and select **Set Cache Flush Interval**.
3. In the Cache Flush Interval field on the dialog box, enter the value (in minutes) of the interval and press **Finish**.
4. Click **OK** on the dialog box that indicates that the command was successfully requested.

Read-load (LUN Load) Balancing

When you enable read-load (LUN load) balancing, read operations on duplex RDR virtual disks alternate between the two physical disks, which improves performance. By default, read-load balancing is enabled on all RDR physical disks.

You can enable or disable read-load balancing either for each physical disk or globally, for all RDR physical disks across the system.

To enable or disable read-load balancing for a single physical disk

1. In ftSMC, expand **ftServer (Local)** and **Logical Disk Information**.
2. Right-click the target **RDR Virtual Disk**.
3. Select **Set Rdr Lun Load Balancing**.
4. In the dialog box, set the **Rdr Lun Load Balancing** field to **On** or **Off**, and click **Finish**.

To enable or disable read-load balancing globally

1. In ftSMC, expand **ftServer Drivers**, right-click **SCSI Port Duplex Driver - Sradisk_Driver**, and select **Properties**.
2. On the dialog box, click the right-most **Properties** tab.
3. In the **GlobalRdrPlexLoadBalancing** field, select **On** or **Off**, and click **OK**.

NOTE

Global read-load balancing settings do not overwrite read-load balancing settings on individual RDR physical disks. So, for example, if the **Lun Load Balancing** field for

a particular RDR physical disk is set to Off, you must set it to **On** before a global load-balancing command can take effect on that disk.

Mirroring Dynamic Disks with RDR

This procedure explains how to turn dynamic disks into basic disks before mirroring them with RDR. To use RDR to mirror dynamic disks themselves, see Chapter 3 in the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).

Mirroring a dynamic disk with RDR involves two steps:

- Converting the disk to basic
- Upgrading the disk to RDR

Converting a Dynamic Disk to a Basic Disk

CAUTION

Converting a dynamic disk to a basic disk removes all data from the disk. Before you convert the disk to a basic disk back it up so that you can recover the data.

1. Go to Computer Management.
2. Expand **Storage** and click **Disk Management**.
3. Right-click the icon of the target disk in the lower portion of the Disk Management details pane.
4. Select **Convert to Basic Disk**.
5. If necessary, recover the information from backup media.

To upgrade the basic disks to RDR, see “Mirroring Disks Using RDR” on page 4-6.

Setting the Active RDR Disk (Plex)

The **Set As Active RDR Plex** command makes the physical disk on which this command is issued the "active" disk. The active disk is the disk:

- From which data is read
- From which a partner disk is resynchronized
- That survives a failover (the failure of one of two, duplex components)
- To which the data traffic goes when disk utilities, like **chkdsk**, are run

You might use **Set As Active RDR Plex**, for example, when using the **chkdsk** command to check the performance of a particular physical disk in an RDR virtual disk. To do this, issue the **Set As Active RDR Plex** command for the physical disk you want to check; this makes it the active disk. Then disable read-load balancing on the RDR virtual disk, and run **chkdsk** on the active disk.

In the following procedure, *n* indicates a component number that appears in ftSMC.

1. In ftSMC, expand **I/O Enclosure - 10** (or **11**), **Storage Enclosure - 40**, **Slot - *n***, and then right-click on **Disk - *n***.
2. Select **Set As Active RDR Plex**.

A message reports that the operation was successful.

Deleting the RDR Configuration on a Physical Disk

Deleting the RDR configuration removes a physical disk from the RDR virtual disk. You delete one physical disk at a time.

After you delete the RDR configuration on a physical disk:

- The RDR metadata is deleted, but other data remains on the disk.
- The disk is no longer an RDR disk and is not part of an RDR virtual disk.
- You can reconfigure the disk as an RDR disk again, using the **Add Physical Disk To RDR Virtual Disk** command.

NOTE

If you delete the RDR configuration from a simplex data disk, then all the New Technology File System (NTFS) partitions on that data disk lose their drive letters.

You can delete the RDR configuration only from basic data disks, but not from simplexed or duplexed boot disks, dynamic disks, or data disks with one or more paging files.

To delete the RDR configuration on a physical disk

1. In ftSMC, expand **I/O Enclosure - 10** (or **11**), **Storage Enclosure**, **Slot - *n***, and then right-click on **Disk - *n***.
2. Select **Delete RDR Configuration on Physical Disk** for disk 0 (or 1 or 2).
3. Optionally, repeat steps 1 and 2 on the disk with which the deleted disk was mirrored.

   When the second of the mirrored disks is removed from the RDR virtual disk, the RDR virtual disk is removed.

4. Repeat steps 1–3 for each physical disk to be removed.

NOTE

Disregard any “Unsafe Removal of Device” messages that appear when you remove an internal physical disk from the enclosure.

Changing Automount Behavior

After you use **Delete RDR Configuration on Physical Disk** on a Windows Server 2008 system, the target disk will appear with a new drive letter in the Windows Disk Manager in Computer Management. This is because Windows Server 2008 uses automounting by default. (On a Windows Server 2003 system, the drive letter is simply deleted.)

To disable automounting in Windows Server 2008, so that it matches the behavior of Windows Server 2003, open a command prompt and issue the following command:

mountvol /n

The change takes effect immediately.

To return the system to automounting, issue the following command:

mountvol /e

Removing a Physical Disk from an RDR Virtual Disk

CAUTION

Removing a physical disk from an RDR virtual disk deletes all of the data from the target disk.

Executing the **Remove a Physical Disk from RDR Virtual Disk** command on a partnered (duplex) RDR virtual disk (comprising two physical disks):

- Erases all of the data on the disk, including all Windows Disk Management dynamic disk metadata and all RDR metadata.
- Returns the physical disk to a basic, non-RDR-configured, blank disk.

The system does not warn you when you issue this command because the target disk has a surviving partner physical disk that still contains all of the data. For that reason, the system does not need to restart.

If you execute the **Remove a Physical Disk from RDR Virtual Disk** command on an unpartnered (simplex) RDR virtual disk (comprising one physical disk), the system

prompts you to remove all partition and volume data on the disk before the command can continue. The prompt alerts you that this operation may result in the loss of all data on this virtual disk since there is only one physical disk.

You cannot remove:

- The only unmirrored boot disk
- The only unmirrored disk containing a paging file
- An unmirrored disk containing data
- A resynchronizing disk

To remove a physical disk from an RDR virtual disk

1. In ftSMC, expand **I/O Enclosure - 10** (or **11**), **Storage Enclosure**, **Slot - *n***, and then right-click on **Disk - *n***.
2. Select **Remove Physical Disk from RDR Virtual Disk**.

Deporting a Physical Disk from an RDR Virtual Disk

Deporting a physical disk from an RDR virtual disk makes the deported disk a clone of its RDR virtual disk partner. You use the **Deport Physical Disk from RDR Virtual Disk** command to create backup disks and spare, bootable, RDR virtual disks.

Once a disk is deported, it is hidden from the system and is inaccessible from ftSMC. It does not become accessible again until you remove it from and reinsert it into the system. You can physically remove and then reinsert the disk, or you can issue the **InitiateBringdown** and **InitiateBringup** commands for the disk slot.

If you insert a disk deported from one system into another system, the disk appears in ftSMC as *Active*, *Configured*, *Deported*.

A deported disk inadvertently left in the system or reinserted into its original slot remains an intact backup. It is not automatically resynchronized or overwritten by the primary RDR virtual disk.

You cannot deport:

- The last physical disk of an RDR virtual disk if it is bootable or contains a paging file
- An unmirrored boot disk
- A dynamic disk
- A resynchronizing disk

The Deport a Physical Disk from an RDR Virtual Disk command should be grayed out if the physical disk is not in the valid state (for example, if it is a dynamic disk or a

simplex boot disk) for this command to work properly. A valid deport operation should rarely fail.

If the Deport a Physical Disk from an RDR Virtual Disk operation requires that the system reboot, a system-restart dialog box appears, giving you the option to restart the system immediately or later. If the operation succeeds without requiring a reboot, a message box indicating success appears.

If Deport a Physical Disk from an RDR Virtual Disk fails, a dialog box indicating the reason for the failure appears. In this case, the RDR virtual disk is not deported and the system does not reboot.

After a successful Deport a Physical Disk from an RDR Virtual Disk command, no drive letters or mount points associated with volumes on the deported disk are preserved.

To deport a physical disk from an RDR virtual disk

1. In ftSMC, expand **I/O Enclosure - 10** (or **11**), **Storage Enclosure- 40**, **Slot - *n***, and then right-click on **Disk - *n***.
2. Select **Deport Physical Disk from RDR Virtual Disk**.

   A message reports that you may have to reboot the system if you continue with this command. You must restart only if the deport command fails. If it succeeds, a message reports the successful operation.

3. Click **OK**.

   A message appears, telling you to remove the deported disk.

4. Remove the deported disk.

The deported disk disappears from ftSMC.

Creating a Spare Bootable RDR Disk

1. Be sure that the system (boot) disk is mirrored.
2. Deport the disk that is the mirror of the system disk, as described in "Deporting a Physical Disk from an RDR Virtual Disk" on page 4-15.
3. Physically remove the deported disk from the system.

   Label and store this disk, which is now the spare bootable hard disk, in a safe place.

CAUTION

If the original boot disk is still in a system into which you insert a spare (deported) boot disk, the original boot disk

loses its RDR configuration and is no longer an RDR-enabled disk.

For more details, see the discussion of creating a spare bootable disk in the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).

Breaking a Physical Disk from an RDR Virtual Disk

The following procedure isolates an RDR virtual disk plex for backup, backs up the volumes, and then resynchronizes the broken plex with its original partner, adding it back to the RDR virtual disk.

You cannot perform this procedure on:

- Dynamic disks
- Simplex RDR virtual disks
- RDR virtual disks while they are resynchronizing
- RDR virtual disks if their verify interval is set to 0; that is, if RDR verify is disabled.

1. Verify the RDR virtual disk that you are going to backup to ensure that both plexes of the RDR virtual disk are healthy.
2. In ftSMC, expand **I/O Enclosure**, **Storage Enclosure - 40**, and then select Slot 1, 2, or 3 to access Disk 0, 1, or 2.
3. Right click on the target disk and select **Break Physical Disk from RDR Virtual Disk**.

   This command splits the plex from the RDR virtual disk, creates an exact copy of its volumes, and adds them to Disk Management.

4. Use backup software to make a copy of these volumes created in Disk Management; then remove the volumes from Disk Management.
5. To add the removed plex back to the RDR virtual disk, in ftSMC, right-click the disk you broke in step 2, and select **Add Physical Disk to RDR Virtual Disk**. See "Adding a Physical Disk to an RDR Virtual Disk" on page 4-7 for the procedure to add a disk.

   The plex is now synchronized with its active partner and is again a partner in an RDR virtual disk.

Setting or Clearing the MTBF for Disks

Clearing the MTBF resets the MTBF to infinity, the number of faults to 0, and the time of last fault to never.

Setting the MTBF Threshold sets the MTBF threshold and views the current count (seconds), number of faults, and date and time of last fault. Stratus presets the MTBF threshold; you should not change it unless instructed to do so by your support representative.

See "MTBF Statistics" on page 5-2 for more information about MTBF.

To set or clear the MTBF for disks

1. In ftSMC, right-click the target disk.
2. Select either **Set MTBF Threshold** or **Clear MTBF.**

   - If you select **Set MTBF Threshold**, specify the desired threshold value in the **Threshold** field of the dialog box that appears, and then click **Finish**.

     A message appears, indicating a successful operation.

   - If you select **Clear MTBF**, the MTBF is cleared and a message appears, indicating a successful operation.

Setting the Hard MTBF Threshold

The **Set Hard MTBF Threshold** command determines the number of seconds the system waits before restoring a failed disk to service. The default is 2 seconds. Generally, retain this setting.

1. In ftSMC, expand **ftServer (Local)**, **ftServer I/O Enclosures**, **I/O Enclosure - 10** (or **11**), **Storage Enclosure - 40**, **Slot - *n***, and right-click the target disk.
2. Right-click on a disk and select **Set Hard MTBF Threshold**.

   The default is two seconds. Although you can set a new threshold, you generally retain the default.
3. Enter the number of Threshold seconds and click **Finish**.
4. Then click **OK** on the dialog box that indicates that the command was successfully requested.

Setting the MTBF Faultcount Limit

The MTBF Faultcount Limit property defines the number of times certain errors can occur before the system sends threshold events that generate alarms.

CAUTION

Do not change the MTBF Faultcount Limit value, except when advised to by the CAC.

To set the MTBF faultcount limit

1. In ftSMC, expand **ftServer (Local)**, **ftServer I/O Enclosures**, **I/O Enclosure - 10** (or **11**), **Storage Enclosure - 40**, **Slot - *n***, and right-click the target disk.
2. Select **Set MTBF Faultcount Limit**.
3. In the dialog box, enter the desired limit value and click **Finish**.
4. Click **OK** on the dialog box that indicates that the command was successfully requested.

Setting the Soft MTBF Threshold

The **Set Soft MTBF Threshold** command determines the number of seconds the system waits before restoring a failed disk to service. The default is 2 seconds. Generally, retain this setting.

A *soft* MTBF refers to disk failures that are not usually fatal to disk operations.

1. In ftSMC, expand **ftServer (Local)**, **ftServer I/O Enclosures**, **I/O Enclosure - 10** (or **11**), **Storage Enclosure - 40**, **Slot - *n***, and right-click the target disk.
2. Right-click on a disk and select **Set Soft MTBF Threshold**.

   The default is two seconds. Although you can set a new threshold, you generally retain the default.
3. Enter the number of Threshold seconds and click **Finish**.
4. Click **OK** on the dialog box that indicates that the command was successfully requested.

Clearing MTBF Settings

Clearing the MTBF sets the MTBF (the current average) to 0 (Unknown) and erases the record of all faults.

1. In ftSMC, expand **ftServer (Local)** until you locate the target component.
2. Right-click the target component and on the shortcut menu, click **Clear MTBF**.

NOTE

Clearing the MTBF does not bring a device back into service automatically.

If the state of device that you cleared is Broken, correct the state.

User actions that can cause the broken state to change include the **Initiate BringUp** and **Initiate BringDown** commands, and removing the board.

Booting a System with a Backup RDR Boot Disk

1. Remove power from the system.
2. Remove all boot disks from the internal storage enclosure, if any are installed.
3. Insert the backup boot disk.
4. Press the system power button.

Reusing Data Disks

If you have stored a copy of a data disk that was created with RDR disk mirroring, use the following procedures to reuse the disk in the system.

Reusing a Stored-Data Disk

After you perform this procedure:

- The data on the stored-data disk is overwritten with the data on the disk in its companion slot.
- The stored-data disk remains an RDR disk.

To reuse a stored-data disk

1. Make sure the original partner of the stored disk is in the companion slot.
2. Insert the stored disk into its original slot. The system automatically resynchronizes the stored disk with the partner disk.

Wait for the disk to be fully resynchronized before removing the stored disk or before removing power from the system.

Removing the RDR Configuration from a Stored-Data Disk

This procedure removes the RDR configuration from a stored-data disk and deletes all of its data.

NOTE

To delete the RDR configuration from a stored-data disk but retains its data, see "Deleting the RDR Configuration on a Physical Disk" on page 4-13.

1. Make sure no disk occupies the slot that is the partner slot to the disk whose RDR configuration you are removing.
2. *If your disk was a dynamic disk*, use your disk-management tool to convert the disk to basic, deleting all data on the disk.

   If your disk was a basic disk, use your disk-management tool to delete all volumes and partitions.

3. In ftSMC, select and right-click the disk, and click **Remove Physical Disk From RDR Virtual Disk**.

CAUTION

You must complete the final step. Otherwise, if the former RDR virtual disk partner of the newly erased disk is inserted into the partner slot of the erased (but not deleted) disk, the newly inserted disk is mirrored to the empty disk, deleting the data on the newly inserted disk.

Resynchronizing RDR Disks

The system automatically resynchronizes disks that are reinserted into the system and when I/O elements are returned to service. In addition, two explicit methods in ftSMC can initiate resynchronization of the physical disks of an RDR virtual disk:

- Resynchronize This Physical Disk From RDR Virtual Disk. This command resynchronizes the chosen physical disk with its with partner.
- Resynchronize Physical Disks Of This RDR Virtual Disk. This command simply makes the two physical disks of an RDR virtual disk identical. The software arbitrarily chooses which disk to make the master and which the copy, irrespective of which disk was last written to.

While the disks are resynchronizing, the disk LEDs blink to indicate read and write operations. You can also use ftSMC to monitor the status of the resynchronization process.

To monitor the status of the resynchronization process

1. In ftSMC, expand **ftServer (Local)**, **ftServer I/O Enclosures**, and **Logical Disk Information**.
2. Click one of the **RDR Virtual Disk** nodes.
3. Check the value of the **Status** property, which displays **Resync *nn*% (**where *nn* is the percentage completed) while the disk is resynchronizing.

When the resync process is finished, the **Status** value for the RDR virtual disk is **None**, and the LED on each physical disk in the RDR pair is lit steady green

When RDR disks are resynchronizing, the Logical to Physical Mapping details pane shows the disk that is resynchronizing as `SYNCING`, and shows the partner disk as `SIMPLEX`.

NOTE

If you insert a blank disk into the companion slot of an RDR virtual disk, the blank disk is automatically configured and synchronized to the existing RDR disk.

Using Resynchronize This Physical Disk From RDR Virtual Disk

To resynchronize a targeted RDR physical disk with its partner

1. In ftSMC, expand **ftServer (Local)** and click **Logical Disk Information**.
2. Right-click the target RDR virtual disk, that is, the disk that might not be synchronized with its mirror disk.
3. Select **Resynchronize This Physical Disk From RDR Virtual Disk**.

   A message appears, indicating a successful start of the command.

See "Disk Failures During Resynchronization" on page 4-10 for instructions on what to do if the source RDR virtual disk fails during resynchronization.

Using Resynchronize Physical Disks Of This RDR Virtual Disk

To resynchronize RDR physical disks to guarantee that they are identical

1. In ftSMC, expand **ftServer (Local)** and click **Logical Disk Information**.
2. Right-click the target RDR Virtual Disk and select **Resynchronize Physical Disks Of This RDR Virtual Disk**.
3. Click **OK** on the dialog box that indicates that the command was successfully requested.

   As shown in the RDR Virtual Disk icon and in the OpState: State property, the RDR Virtual Disk changes from Duplex to Simplex.

   When resynchronization completes, the RDR Virtual Disk changes from Simplex to Duplex, as shown in the RDR Virtual Disk icon and the OpState: State property.

Resynchronizing a Backup Boot RDR Disk

To automatically resynchronize a partner RDR physical disk by insertion

1. Verify that the original partner disk of the backup boot disk is inserted into its original slot in the storage enclosure.
2. Reinsert the backup boot disk into its original slot in the storage enclosure.

   The backup boot disk automatically resynchronizes with the original partner. The command takes some time to run.

Recovering and Replacing RDR Disks

In your disk-management tool, if the status of an RDR disk appears as **Offline**, **Missing**, or **Online (Errors)**, you can try to recover the disk manually. Verify that the disk is securely seated in the enclosure and that it has power. Perform the following procedures to recover the disk.

To recover an RDR disk

1. Delete the RDR configuration on the disk and then physically remove it from the enclosure.

   NOTE

   Disregard any "Unsafe Removal of Device" messages that appear when you remove an internal physical disk from the enclosure.

2. Replace the defective disk and add the disk to an RDR virtual disk.

In the unlikely event of a system failure resulting from disk failures, restore the system by performing one of the following procedures, as appropriate:

- Restore the system by using a backup system disk. See the discussion of creating spare bootable hard disks in the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) for information.
- Reload the ftServer System Software, as described in the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).

To replace a failed physical RDR disk

1. Remove the failed disk.
2. Insert a blank replacement disk.

Verifying RDR Disks

RDR disk verification verifies the integrity of RDR disk mirrors. Specifically, it:

1. Reads all sectors on both disks. If it detects a read error, it recovers the degraded sector from the good partner disk. This safeguards the integrity of both disks.
2. Compares the data from each sector on both disks. If it detects a discrepancy, it logs an error to the event log. In the unlikely event that this happens, contact the CAC or your authorized Stratus service representative, or log an issue under their maintenance contract.

To verify an RDR disk

1. In ftSMC, expand **ftServer (Local)** and click **Logical Disk Information**.
2. Right-click the appropriate RDR virtual disk.
3. Select **Verify RDR Virtual Disk**.

A message appears, stating that the operation completed successfully.

To stop verifying an RDR disk

Use the following procedure to stop RDR verification.

1. In ftSMC, expand **ftServer (Local)** and click **Logical Disk Information**.
2. Right-click the appropriate RDR virtual disk.
3. Select **Stop Verify RDR Virtual Disk**.

A message appears, stating that the operation completed successfully.

To set the interval for automatic RDR disk verification

1. In ftSMC, expand **ftServer Drivers**, right-click **SCSI Port Duplex Driver - Sradisk_Driver**, and select **Properties**.
2. In the dialog box, click the third **Properties** tab from the left.
3. Set the **LunVerifyInterval** property to the desired value and click **OK**.

   The default value is 10080 minutes (7 days), meaning 10080 minutes from the time of the last verification command. The nonzero minimum value cannot be less than 60 minutes. A value of 0 disables automatic RDR disk verification.

Making Sure You Do Not Boot from a Stale Disk

If the system becomes powered off because power to both enclosures is lost, but not at the same time, RDR disks become unsynchronized. In this case, if you do not use care in rebooting the system, it can boot from a stale disk. If you experience such a power loss to the system, boot from the enclosure that was running most recently (remove the power cord from the other enclosure, whose disks contain stale information). If you cannot be sure which enclosure to boot from, contact the Stratus Customer Assistance Center (CAC) or your authorized Stratus service representative for help.

You may need to recover updated data if your applications start to run on a stale disk.

When you are sure that the system and data disks on the boot enclosure are updated, restore power to the second enclosure.

Configuring the Priority of RDR Virtual Disk Resynchronization

The resynchronization priority establishes the portion, expressed in megabytes per second (Mbps) in the details pane, of I/O bandwidth that is used for the RDR disk resynchronization operation.

To prioritize resynchronization for all RDR disks in the system

1. In ftSMC, expand **ftServer Drivers**, right-click **SCSI Port Duplex Driver - Sradisk_Driver**, and select **Properties**.
2. In the dialog box, click the third **Properties** tab from the left.
3. Set **GlobalResyncPriority** to **Low**, **Normal**, or **High** and click **OK**.

To prioritize resynchronization for individual RDR disks

1. In ftSMC, expand the appropriate I/O Enclosure node and click **Logical Disk Information**.
2. Right-click the target RDR virtual disk.
3. Select **Set Resync Priority**.
4. Select **Low**, **Medium**, or **Normal** and click **OK**.

Using Volume Mirroring for Fault Tolerance

You can use Windows Disk Management to mirror volumes on disks in internal storage subsystems.

When using Windows Disk Management to implement data fault tolerance, format volumes as NTFS volumes.

- Configure disks as *dynamic* disks. Dynamic disks organize data within volumes on a disk and support fault-tolerant operation and disk migration between systems.
- Mirror each volume (the boot volume on the system disk and all data volumes) on two or more physical disks. See "Mirroring Disks in ftScalable Storage Systems" on page 4-29 for details.
- Assign system disks and data disks to the same disk group.

CAUTION

Failure to set up your disk storage as required results in storage that is not fault tolerant.

A *mirror* is an identical copy of data that you can access if your primary data becomes unavailable. Stratus requires that you mirror the boot volume on the system disk. The resulting mirrored pair of disks work together to provide a fault-tolerant volume. If one disk fails, the volume automatically uses the data from the other disk.

Mirror all data volumes. Mirroring volumes as documented provides fault tolerance, because volumes are mirrored on separate physical disks on separate FC buses.

When mirroring volumes, pair identical physical disks (same capacity, model, and manufacturer) so that in the event of a disk failure, an entire physical disk can be replaced without any data loss. See "Mirroring Disks in ftScalable Storage Systems" on page 4-29 for details.

Mirrored Volume Resynchronization

When a volume is mirrored across two physical disks, and one of the disks fails or is brought offline for any reason, the remaining good disk continues to operate. However, the data on the mirrored volumes is no longer synchronized.

After a disk is replaced or brought back online, the mirror between it and the disk that remained in operation must be resynchronized. During resynchronization, the system copies the format and the contents of the good mirrored volume(s) to their mirror(s) on the disk most recently brought back online.

NOTE

Because mirror resynchronization can severely affect performance, you should resynchronize mirrors when the system is least busy.

Mirror resynchronization can occur automatically, or, in some cases, you must resynchronize the mirror manually:

- If you insert a replacement disk without a disk signature into the same slot as the failed disk, the system automatically attempts to resynchronize the disk.
- If you replace a failed disk with a blank basic or dynamic disk that contains a signature, you must resynchronize the disks manually.
- The system automatically attempts to resynchronize the disks if:
  - An I/O element is removed and inserted.
  - An I/O element goes offline and returns online.

Volume Resynchronization After Rebooting

After rebooting the system, and depending on the circumstances under which the system was shut down, you may need to explicitly reactivate a failed mirrored partner to resynchronize a volume.

For example, if the system was shut down normally, but it was shut down while synchronization was in progress, you need to explicitly reactivate the mirror. On the

other hand, if the system shutdown was due to an unexpected event like a power failure, the disks begin the remirroring process automatically after booting.

Before mirroring system disks with a disk management tool, make sure either that both disks are plexes of an RDR virtual disk or that neither disk is. Do not partner RDR and non-RDR system disks in a mirror. Otherwise, the disks will fully resynchronize after every reboot.

The boot disks do not require resynchronization if the RDR disk is the primary boot volume from which the system is booted.

NOTE

You may remove disks from or insert disks into the internal storage as needed.

Using Hardware RAID Controllers For Fault Tolerance

Optional ftScalable Storage systems employ redundant hardware RAID controllers. Fault-tolerant volumes reside on virtual disks configured in a supported RAID topology. Use the embedded RAIDar graphical user interface to create and configure the virtual disks. You use Windows Disk Management to create the volumes. See the *ftScalable Storage: Getting Started Guide* (R601) and the *ftScalable Storage: Operation and Maintenance Manual* (R600) for information about how to create, configure, and monitor fault-tolerant disk resources on ftScalable Storage systems.

ftSMC Interface for Storage Enclosures and Subsystems

The Storage Enclosure - 40 node represents the internal storage subsystem, and the **ftScalable™ Storage** node represents ftScalable Storage systems. It appears only on systems to which ftScalable Storage is attached.

EMC® attached storage systems are not directly represented in ftSMC. The Fibre Channel Controller node represents the adapter associated with an attached EMC storage subsystem.

Storage Enclosure Node

The **Storage Enclosure** node contains the following two nodes:

- Slot
- Disk

Slot Node

The **Slot** node represents the slots where disks reside. System disks must reside in certain slots (see "Mirroring Disks in ftScalable Storage Systems" on page 4-29 for details).

NOTE

In ftSMC, the storage **Slot** nodes display the **Start Slot Identification** and **Stop Slot Identification** commands. Although these commands appear in the context menu for slots in internal storage, the driver for those slots does not support them.

Disk Node

Each **Disk** node represents a hard disk that resides in a slot in a storage enclosure. You use the DevicePathID property to locate a physical disk. See "Finding an Internal Physical Disk" on page 4-29 for details.

ftScalable Storage

If your system contains an optional ftScalable Storage system, **ftScalable™ Storage** and **ftScalable™ Storage Controller** nodes appear beneath the **Storage Enclosures** node. Also **Fibre Channel Controller** nodes that appear beneath the **PCI Slot Info** nodes represent the PCI adapters associated with the ftScalable Storage system.

NOTE

System disks cannot reside in an ftScalable Storage system.

EMC Attached Storage

If an EMC CLARiiON® or EMC Symmetrix® storage system is installed in your system, **Fibre Channel Controller** nodes that appear beneath the **PCI Slot Info** nodes represent the PCI adapters that connect the ftServer system to the EMC storage system.

NOTE

System disks cannot reside in an EMC attached storage system. See "Mirroring Disks in ftScalable Storage Systems" on page 4-29 for details.

The values that the Op State: State and Op State: Reason properties can take vary depending on whether EMC PowerPath® software is running. See Table 4-2 for details.

Table 4-2. FC Host Bus Adapter State and Reason Property Values

	Op State: State	Op State: Reason
With PowerPath software running	Simplex	None
	Duplex	None
	Broken	Media Disconnect
	Broken	None
Without PowerPath software running	Online	None
	Broken	Media Disconnect

When you reattach a cable between your EMC storage system and the PCI adapters in your system, the connection state may not be immediately reflected in ftSMC. To update ftSMC, issue the command `powermnt restore` in PowerPath, from **Run** on the **Start** menu, or from a command prompt. The information in ftSMC will update in about 15 seconds.

Mirroring Disks in ftScalable Storage Systems

ftScalable Storage systems include hardware RAID controllers. Use the embedded RAIDar graphical user interface to create and configure fault-tolerant virtual disks and volumes. See the *ftScalable Storage: Getting Started Guide* (R601) for more information.

Finding an Internal Physical Disk

You can locate internal physical disks by using either the Logical to Physical Mapping node or the Disk node (beneath Storage Enclosure - 40, Slot - n).

To use the Logical to Physical Mapping node

1. In ftSMC, expand **ftServer (Local)** and then **Logical Disk Information**.
2. Click **Logical to Physical Mapping**.

For RDR virtual disks, the detail pane presents information in the following format:

```
Harddisk0-LUN1-PLEX2 (Basic) 11/40/1 (DUPLEX)
Harddisk0-LUN1-PLEX1 (Basic) 10/40/1 (DUPLEX)
```

The information for non-RDR disks is the same, except that it does not include LUN (RDR virtual disk) or PLEX (physical disk) information, which pertains only to RDR disks.

In the details pane:

- `Harddisk0` refers to the Windows disk name.
- `LUN1` refers to RDR virtual disk 1. The system assigns the LUN numbers dynamically. (An ftServer system can support a maximum of three RDR virtual disks.)
- `PLEX1` and `PLEX2` refer to the two physical disks that together make up RDR virtual disk 1 (LUN 1).
- `Basic` refers to type of disk. The other possible value is `Dynamic`.
- `10/40/1` indicates the following:
  - `10` indicates I/O element 10.

    NOTE

    In rack-mounted systems, I/O element 10 is in the top enclosure and I/O element 11 is in the bottom enclosure. Pedestal systems are rotated 90 degrees **clockwise** (viewed from the front), so that I/O element 11 is on the left side of the system and I/O element 10 is on the right side.

  - `40` indicates the internal storage enclosure within the I/O element.
  - `1` indicates the top disk slot in rack-mounted systems.
- For RDR disks, `Duplex` indicates that the two physical disks of the RDR virtual disks are partnered. If the two physical disks were not partnered, the displayed value would be `Simplex`.

  For non-RDR disks, the values in this position indicate the disk's operating status.

RDR virtual disks also appear in ftSMC under the Logical Disk Information node. In this location, the details pane presents the location of the physical disks in the RDR virtual disk in these properties:

- Disk Enclosure Slot: DevicePath[2]
- Disk Enclosure Slot: DevicePath[1]

However, the DevicePathID property that appears at the top of the details pane, and which has a number like 39/7, does not indicate a hardware component and does not signify the physical disks's location in the system; it merely identifies the virtual disk to system-management software.

To use the Disk node

1. In ftSMC, expand **ftServer (Local), Storage Enclosure - 40**, and **Slot - n**.
2. Click **Disk - n**.

The location of the disk appears in the DevicePathID property, which presents the location information similar to the following: 10/40/1/0. This DevicePathID indicates the following:

- 10 indicates the I/O element number
- 40 indicates internal Storage Enclosure - 40
- 1 indicates the disk slot number
- 0 indicates the disk number

Finding an External Physical Disk

To find an external disk in your ftScalable Storage system, see the description of the **set led** command in the *ftScalable Storage: Commands Reference Manual* (R599).

See the *ftScalable Storage: Getting Started Guide* (R601) and related documentation for information about ftScalable Storage.

The disks of EMC storage systems do not appear in ftSMC.

Chapter 5
Troubleshooting

The following topics can help you troubleshoot your ftServer system:

- "MTBF Statistics" on page 5-2
- "Taking Components Offline and Bringing Them Online" on page 5-3
- "Expansion ROM Console Message During System Boot" on page 5-3
- "Hard Disks" on page 5-3
- "Determining That a Component Has Failed" on page 5-6
- "Locating Components" on page 5-7
- "When Windows Does Not Respond" on page 5-9
- "Delayed System Restart" on page 5-9
- "Unresponsive Mouse and Keyboard" on page 5-9
- "Remote Event Notification and Service" on page 5-10
- "Making Dump Files" on page 5-12
- "Disaster Recovery" on page 5-14
- "Windows Hotfixes Distributed by Stratus" on page 5-16
- "Adaptec SAS Controller BIOS RAID Option" on page 5-17
- "Tape Drivers and Backup on Windows Server 2008 Systems" on page 5-17

NOTE

See the sections on reviving a nonresponsive system and the various diagnostic codes in the *Stratus ftServer Virtual Technician Module User's Guide* (R642) for more information on troubleshooting a system.

MTBF Statistics

The fault-tolerant services software automatically maintains mean-time-between-failure (MTBF) statistics for many system components. Administrators can view this information in ftSMC and can reconfigure the MTBF parameters that affect how the fault-tolerant services respond to component problems.

The system stores the current MTBF values associated with each device in Windows registry keys. Whenever an MTBF value changes, the registry reflects the change. Therefore, when the driver stops and restarts, or the system restarts, the system retains the current MTBF information.

For procedures explaining how to set these settings, see ftSMC Help.

Clearing the MTBF

Clearing the MTBF sets the MTBF to 0 (Unknown) and erases the record of all faults.

NOTE

Clearing the MTBF does not bring a device back into service automatically.

If the device that you cleared is in the Broken state, you must correct the state.

User actions that can cause a transition out of the Broken state include the Initiate BringUp and Initiate BringDown actions and removing the board.

Changing the MTBF Threshold

The MTBF threshold is expressed in seconds. If a device's MTBF falls beneath this threshold, the system takes the device out of service and changes the device state to Broken.

CAUTION

Stratus presets the MTBF thresholds. Do not modify them unless instructed to do so by the CAC or your authorized Stratus service representative.

Taking Components Offline and Bringing Them Online

You can use ftSMC to take a component offline or bring a component online. Before you take a component offline, verify that it is safe to do so. Taking components offline safely is discussed in ftSMC Help.

Expansion ROM Console Message During System Boot

Depending upon the number and types of PCI adapters, some ftServer systems may display the following console message while booting:

```
Expansion ROM not initialized - PCI network adapter in slot xxxx
```

You can safely ignore this message. You can avoid receiving this message by disabling **Option ROM Scan Monitoring** for one or more PCI adapter slots in the **Monitoring Configuration** submenu in the BIOS. See "Managing BIOS Settings" on page 2-11 as well as the *Stratus ftServer Systems: Technical Reference Guide* (R550) for information about how to change BIOS settings.

Hard Disks

If a disk's status is not healthy, you may be able to recover the disk, or you may need to replace the disk.

Recovering a Disk

In your disk-management tool, try to recover the disk manually if:

- A failed volume (non-RDR only) appears as **Failed Redundancy**
- The RDR or non-RDR disks appear as **Offline**, **Missing**, or **Online (Errors)**

Verify that the system does not have a problem that is causing the mirror to break on an internal or external disk. Ensure that the disk is securely seated in the drive and that it has power. Perform the following procedures to recover the disk.

To recover an RDR disk

1. Logically and then physically remove the physical disk from the RDR virtual disk.

   NOTE

   Disregard any "Unsafe Removal of Device" messages that appear when you remove an internal physical disk from the enclosure.

2. Replace the defective disk and make the disk an RDR disk, as described in "Mirroring Disks Using RDR" on page 4-6.

In the unlikely event of a system failure resulting from disk failures, restore the system by performing one of the following procedures, as appropriate:

- Restore the system by using a backup system disk. See the discussion of creating spare bootable hard disks in the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) for information.
- Reload ftServer System Software (ftSSS), as described in the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W).

To recover a disk in Windows Disk Management

1. Go to Computer Management and click **Disk Management**.
2. Right-click the disk icon corresponding to the disk that has the **Offline**, **Missing**, or **Online (Errors)** status, and in the option menu, click **Reactivate Disk**.
3. After the mirror regenerates (this may take several minutes), verify that the status of the disk has returned to **Healthy**.

CAUTION

If a disk continues to have the status of **Online (Errors)**, replace it as soon as possible.

If the recovery procedures fail to reactivate the disk, or if the status does not return to **Healthy**, you must physically replace the failed disk.

Replacing a Failed Disk in Windows Disk Management

You can replace a failed disk with an uninitialized disk (a disk that has no signature written on it). This is the quickest and easiest option. If your only spare disk is initialized (it has a signature written on it), you can replace the failed disk with an initialized disk.

Replacing a Failed Disk with an Uninitialized Disk

Follow this procedure to replace a failed disk with an uninitialized disk. To physically locate a disk, see “Finding an Internal Physical Disk” on page 4-29.

To replace a failed disk with an uninitialized disk

1. Physically remove the failed disk and replace it with an uninitialized disk.
2. Disk-management software automatically resynchronizes the replacement disk with the remaining good disk, creating volumes on the replacement disk and mirroring the disks.

Replacing a Failed Disk with an Initialized Disk

Perform the following procedure to replace a failed disk with an initialized disk using Windows Disk Management.

To use Windows Disk Management to replace a failed disk with an initialized disk

1. Physically remove the failed disk and replace it with an initialized disk. For details, see the operation and maintenance guide for your system.
2. Examine the type of the initialized replacement disk:
   - If the replacement disk's type is **Foreign Dynamic**, go to step 3.
   - If the replacement disk's type is **Basic**, go to step 4.
3. In Disk Management, right-click the foreign dynamic replacement disk, and then click **Convert to Basic**. The replacement disk should now appear as a basic disk.
4. If the basic replacement disk has any volumes, delete them. Right-click the volume on the replacement disk, and then click **Delete Partition**. Repeat for each volume on the replacement disk. Verify that the basic replacement disk now appears as a single unallocated space.
5. Right-click the replacement disk and click **Convert to Dynamic**.
6. Remove the mirrors from the missing disk that was physically removed in step 1. Right-click a volume on the missing disk and then click **Remove Mirror**. In the **Remove Mirror** dialog box, select the missing disk and click the **Remove Mirror** button.

   CAUTION

   Be sure to select the missing disk, not the remaining good disk. You will lose data if you select the remaining good disk.

   Repeat this step for each volume on the missing disk.
7. Right-click the missing disk, and then click **Remove Disk**.
8. On the remaining good disk, right-click a volume and click **Add Mirror**. In the **Add Mirror** dialog box, select the replacement disk and click the **Add Mirror** button. Repeat this step for all other volumes on the remaining good disk.

Hardware Installation Wizard

Occasionally, after a system reboot or after hot-plugging an I/O element or a disk, a hardware-installation wizard may appear, indicating that a "Stratus disk device" has been found. Continue through the wizard steps, but click **Cancel** at the end rather than rebooting.

Determining That a Component Has Failed

Component LEDs and ftSMC provide indicators that a component has failed. See the operation and maintenance guide for your system for general troubleshooting information related to system hardware. ftSMC indicates a failed component by showing a white X inside a red box ( ) next to the icon of a failed component.

Using LEDs to Troubleshoot Hardware

LEDs indicate the status of their associated components. The enclosure status LEDs are green and amber, and are located on the front and rear of each enclosure.

The enclosure LEDs represent the combined states of the CPU element, I/O element, BMC, the internal disks, and the PCI adapters.

The LED states are described in detail in the hardware troubleshooting chapter of the operation and maintenance guide for your system. See the *ftScalable Storage: Getting Started Guide* (R601) for information about the ftScalable Storage system LEDs.

Using ftSMC to Troubleshoot Hardware

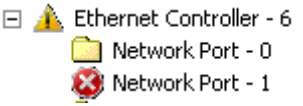
You can view component icons in ftSMC to see if a component has failed.

To use ftSMC to determine that a component has failed

1. In ftSMC, expand the System Inventory by clicking the **ftServer** node in the console tree and pressing the asterisk (*) key on the numeric keypad.
2. Look for **Warning** ( ) or **Error** ( ) icons. If you see a **Warning** icon, click the plus sign (+) in front of nodes that have a **Warning** icon until you see an **Error** icon.

   For example, in Figure 5-1, a **Warning** icon appears in one node, and the **Error** icon appears beside the port that has a problem.

Figure 5-1. Warning and Error Icons



3. Click the problem node and check the `MTBF: Current` value in the details pane. If it is less than the `MTBF: Threshold` value, that node has failed and the system removes it from service. For example:

```
MTBF: Time of Last Fault    May 30, 2008 15:07:24
MTBF: Threshold                 300 seconds
MTBF: Number of Faults          2
MTBF: Current                     220 seconds
```

Locating Components

ftSMC displays device IDs and device paths for system components that it monitors. Component location diagrams show the device IDs of major elements, enclosures, and internal disks. Two commands assist you in locating select system components:

- **Start Slot Identification**. Causes the LEDs on the component to flash so that you can physically locate it.
- **Stop Slot Identification**. Stops the LEDs on the component from flashing after you have physically located it.

CPU-I/O enclosures, PCI adapters, and modems support these slot identification commands.

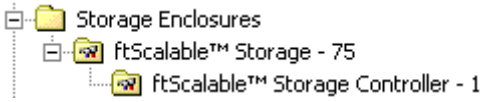
Device IDs and Device Paths

Hardware components in the system inventory are organized hierarchically. Level 1 components (for example, CPU elements and I/O elements, represented by the CPU Enclosure nodes and I/O Enclosure nodes, respectively) have Level 2 child components, such as DIMMs and processors, which may have Level 3 and Level 4 components.

Hardware devices in the system inventory have *device ID* numbers. For example, the device ID of the ftScalable Storage subsystem in Figure 5-2 is 75. The figure illustrates the following hierarchically presented components and their device IDs:

- Level 1: Storage Enclosures (the external storage subsystem)
- Level 2: ftScalable Storage - 75
- Level 3: ftScalable Storage Controller - 1

Figure 5-2. Component Levels



A *device path* is a slash-separated sequence of device IDs that identifies the location of a component in the system. Device paths appear in the details pane of ftSMC. They use the following syntax:

Level-1 device ID/*Level-2 device ID*/*Level-3 device ID*/*Level-4 device ID*

Table 5-1 presents the system device IDs.

Table 5-1. System Device IDs

Device Name(s)	Device ID(s)
Call-Home Modem	0
CPU Enclosure (element) DIMM Processor	0,1 1–12 21 and 22
I/O Enclosure (element) Serial Attached SCSI Controller Ethernet Controller ...Network Port Video Controller USB Controller PCI Slot Info PCI to PCI Bridge Storage Enclosure (internal) ...Slot .....Disk BMC	10, 11 5 6 0,1 7 8, 9 1–4 10 40 1–8 *n* (variable)† 120
ftScalable Storage (optional) ftScalable Storage Controller	75 1
RDR Virtual Disk	*n* (variable)‡

† The Windows operating system assigns these numbers.
‡ Assigned incrementally based on next available number.

Device IDs and device paths apply only to hardware components. Logical devices and software components do not have device IDs even if they appear in the ftSMC interface.

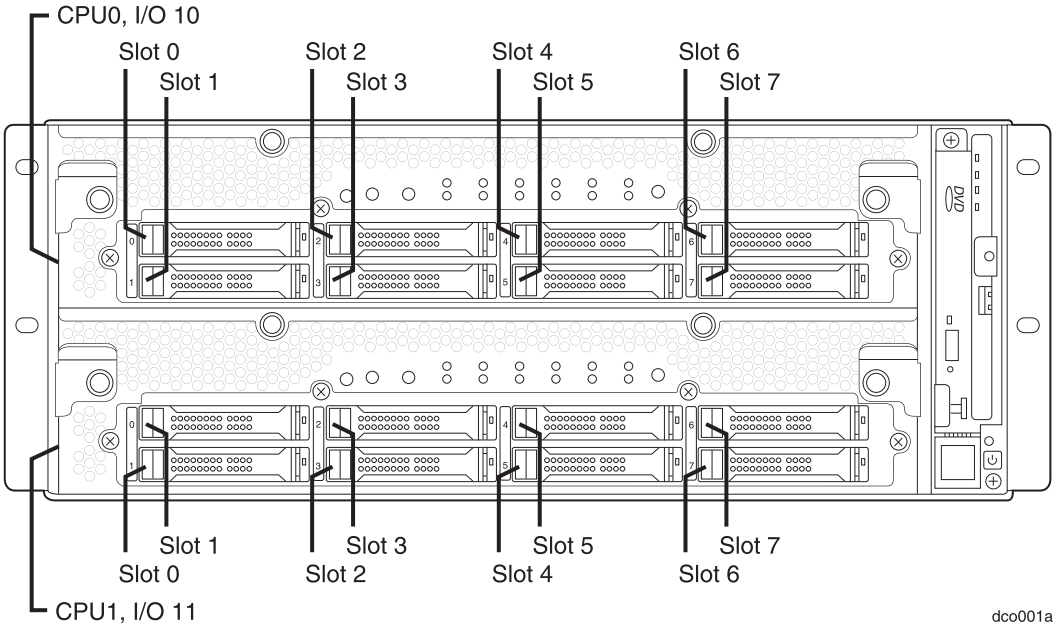
Diagrams of Component Locations

See Figure 5-3 to locate I/O and CPU elements and internal-storage disk slots for your ftServer system. If a component is shown as failed or failing in ftSMC, note its device ID and then use the following information to locate that component within the system. All top-level components have a physical label that includes their device ID.

System Elements and Internal Storage Disk Locations

Figure 5-3 shows the front view of an ftServer 2600, 4500, or 6300 system. It shows the locations of the CPU and I/O elements and disk slots. The internal storage is housed in an enclosure located to the right of the CPU-I/O enclosure.

Figure 5-3. CPU-I/O Enclosure and Disk Slot Labeling



When Windows Does Not Respond

If Windows does not respond (that is, if the system appears hung), use the VTM console or the power button to restart the system. Related information can be found in the *Stratus ftServer Virtual Technician Module User's Guide* (R642).

Delayed System Restart

When you restart a system that contains certain models of adapters, the system appears to hang for approximately 10 seconds while the drivers for the adapter are installed. Allow several seconds for restart to proceed.

Unresponsive Mouse and Keyboard

The mouse and keyboard may appear unresponsive at some point after the system has restarted. This is normal behavior while the operating system finds the virtual mouse and keyboard as new hardware. Responsiveness returns after a short period of time.

Remote Event Notification and Service

The ASN provides the following features:

- Event reporting to your supporting Stratus CAC or your authorized Stratus service representative
- Remote service to your system by service support personnel

You use the ASM Web site to configure all remote event reporting and remote service features of the ASN. See the *Stratus ActiveService Network Configuration Guide* (R072) for details.

Remote Reporting of Events

When the system's fault-tolerant software detects a hardware or software problem, the system generates alarm messages (also referred to as alerts) that can be:

- Sent to the CAC or other authorized Stratus service representative
- Sent to a customer contact by way of email
- Written to the Windows system event log

Alarm Messages

Alarm messages placed in the system event log contain information about device state changes such as changing modes from duplex to simplex, failure of diagnostics on a device, exceeded thresholds, memory dumping, and failed device startups. Alarm messages appear with `Stratus Alarms` as the event source.

You can configure your system to send alarm messages by the following options:

- Internet with phone line as backup
- Phone line with Internet as backup
- Phone line only
- Internet only

Determining the Value of the Send Alarms By Property

1. In ftSMC, expand **ftServer (Local)** and **ftServer Configuration**.
2. Click **ActiveService Network**.
3. In the details pane, check the value of the Send Alarms By property.

See the *Stratus ftServer Systems: Technical Reference Guide* (R550) for descriptions of the alarm messages.

Event Notification on Boot Failure

The VTM will send an alarm when a fault-resilient boot fails to bring up the Windows operating system.

NOTE

Starting with ftServer 2600, 4500, and 6300 systems, VTM functionality is integrated into the baseboard management controller (BMC). In previous ftServer system models, the VTM and BMC were separate hardware components.

System Inventory Reports

An alarm message can include a full system inventory, a partial system inventory, or no inventory at all, depending on the message type. A *system inventory* consists of an enumeration of all of the properties of the manageable hardware devices tracked by the Inventory service.

Event-Log Entries

System software may generate an alarm in response to a sequence of several events. To indicate what these events are, an alarm message may include event-log entries. These event-log entries contain items that represent an event from both the system event logs (SELs) and application event logs (AELs). The number of event-log entries included with an alarm message is determined by specifying how many seconds of the event log to include. System software may configure this time differently for each type of alarm, or it may exclude some event-log entries.

The BMC on each CPU-I/O logs SELs for its CPU-I/O enclosure. The Windows System Manager (WSM) reads the SELs from each BMC and saves them to the AELs. In the AELs, the system events are simply interleaved with one another, not merged, so events reported on both enclosures appear in duplicate.

Remote Service

If you have a service contract with the CAC or your authorized Stratus service representative, your service representative can connect to your system through either the Internet or a phone line.

When the connection is through a phone line, the VTM validates that the phone call is from a permitted source, disconnects the incoming call, and calls back to make a connection to the validated CAC.

You can configure the system to allow the CAC or your authorized Stratus service representative to connect to your system through the Internet, using secure tunneling over IP, to diagnose problems and perform data-transfer functions. These accesses are subject to validation by the CAC database, by the VTM on your system, and by you

as the system administrator. Connecting through the Internet provides higher-speed, more reliable connections than connecting through a phone line.

The CAC or your authorized Stratus service representative may contact you to determine the seriousness of the condition. If a CRU has failed, the CAC or your authorized Stratus service representative will ship a new part to your site.

System software continuously copies a limited number of Windows system event-log messages to a log on the BMC so that support personnel can retrieve the log if your system fails.

Making Dump Files

Dump files are snapshots of either a system's memory or a particular component's firmware memory. Dump files enable the CAC or your authorized Stratus service representative to diagnose system or component problems. You can create dump files in the following ways:

- Press a button
- Configure your system to create memory dumps
- In ftSMC, right-click a CPU Enclosure, and select the Dump and Go command
- In ftSMC, right-click a certain component, and select either the Dump and Go command or the Dump command. (These commands are not available for all components.)
- Use the VTM console

The Dump command dumps a snapshot of the corresponding component. During a dump, the component is not available. When the dump is complete, the component returns to service.

You can also use Windows commands to configure the creation of memory dumps. See Windows documentation.

Using the NMI (Dump) Button

CAUTION

Making a dump file of an entire system automatically takes the operating system offline and then restarts it.

Press the non-maskable interrupt (NMI) button on the primary (active) CPU-I/O enclosure. The *primary enclosure* is the one whose PRIMARY LED is lit. In order to see the PRIMARY LED, you must remove the system bezel. However, you can see the enclosure status in ftSMC. The NMI button is also referred to as the dump button. It is

located on the front of the CPU-I/O enclosure, though it is obscured by a bezel. (See your operation and maintenance guide for details.)

Configuring System Memory Dumps

Memory dumps are enabled through the Board Instance driver's DumpQuickEnabled and DumpNumberOfFilesToSave properties.

To enable system memory dumps

1. In ftSMC, expand **ftServer (Local)**, **ftServer Drivers**, and then **Board Instance Driver - srabid**.
2. Right click **Board Instance Driver - srabid**, select **Properties**, and set **DumpQuickEnabled** to **True**.
3. Set **DumpNumberOfFilesToSave** to the number of dump files you want to save to disk.

   Dump files beyond this number overwrite the existing saved dump files. For instance, if the value is 3, then the fourth saved dump file overwrites the first, existing dump file.

If, at the time of a system crash, the DumpQuickEnabled property of the **Board Instance Driver** node is **True** and the CPU element is duplex, the system creates a memory dump and stores the dump in the memory of one CPU element. The system restarts with the remaining CPU element. After the system restarts, the dump is automatically copied to a disk file.

After a system reboot where a dump has been generated, do not attempt to read or copy the Memory.dmp file created. After the system has completed writing the Memory.dmp file, it renames the file Memory*n*.dmp, where *n* is a numeral. You can read or copy the Memory*n*.dmp file. It may take up to five minutes after the reboot to complete writing the Memory.dmp file before it is renamed and can be read.

CAUTION

If you attempt to read or copy the Memory.dmp file while the system is writing it, you may corrupt the file.

The normal Windows dump mechanism is used if the **DumpQuickEnabled** parameter is **False** (disabled) or if the CPU element is in simplex mode.

Dump and Go

The Dump and Go command captures a snapshot dump of a running system or a particular component without significantly interfering with the system's or component's operation. The system must be running duplex if you use this method.

To capture a snapshot dump, right-click the **CPU Enclosure** node of interest in the ftSMC console tree and select **Dump and Go** from the Action menu. The system:

- Takes the selected CPU element offline with its memory intact
- Dumps a snapshot of the memory to C:\ftSysDump\MEMORY*n*.DMP
- Displays the status of the operation
- Returns the CPU element back to online status

Making a Dump File Using the VTM Console

Perform the following procedure to make a dump file.

1. Start a VTM session on the primary BMC:
   a. In ftSMC, expand **ftServer (Local)**, **ftServer I/O Enclosures**, **I/O Enclosure - 10**, **BMC - *n***.
   b. Copy the IP address of the primary BMC from the ftSMC details pane.
   c. Enter the primary BMC IP address in the **Address** field of an Internet Explorer browser.

   NOTE

   You do not need to be on the primary BMC to perform this procedure.

2. When the VTM login window appears, log in. For information on logging in to the VTM console, see *Stratus ftServer Virtual Technician Module User's Guide* (R642).
3. Click the **Remote Control** tab. On the page that opens, click **Dump**.

   CAUTION

   Making a dump file of an entire system automatically takes the operating system offline and then restarts it.

Disaster Recovery

To help you to log on and access system resources after a computer disaster has occurred, you can restart the system in safe mode or boot from a spare disk.

Safe Mode

You use the Safe Mode startup options to start the system with only the minimal necessary services. Safe Mode options include Last Known Good Configuration, Safe Mode, Safe Mode with Networking, and Safe Mode with Command Prompt. For more information, see Safe Mode startup options in Windows Help.

CAUTION

You must disable the Watchdog Timer by disabling boot monitoring in the BIOS before attempting to boot in Safe Mode. See the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) for a description of how to disable boot monitoring.

Booting From a Spare System Disk

To boot from a spare system hard disk, you need a spare hard disk that was prepared during your initial system configuration process. Refer to the *Stratus ftServer System Software: Installation and Configuration for Windows Systems* (R002W) for information about how to prepare this hard disk. Typically, you boot from a backup hard disk only to recover from an unlikely disaster situation where all redundant system disks suffered simultaneous failure.

To boot a system from an RDR boot disk, see "Booting a System with a Backup RDR Boot Disk" on page 4-20.

The following procedure explains how to boot a system from a non-RDR system disk.

To boot from a previously prepared non-RDR spare system disk

1. Shut down the operating system.
2. Physically remove one of the original system disks.
3. Insert the spare system disk into the empty slot created in step 2.
4. Unlatch the other original system disk.
5. Power up the system.
6. After the system has booted, insert (latch) the original disk that you unlatched in step 4.
7. Use your disk-management tool's **Delete Volume** command to delete the volume on the original disk you inserted in step 6. When this step is complete, the disk is set to **Unallocated space**.
8. Create a mirror of the spare system disk's C: volume on the original disk you inserted in step 6.

   Using Windows Disk Management, right-click the spare system disk's C: volume. In the shortcut menu, click **Add Mirror**. A wizard prompts you through the rest of the mirroring process.

NOTE

When you mirror a system disk, click **OK** when a pop-up window with the following message is displayed: *Windows Disk Manager could not update the boot file for any boot partitions on the target disk. Verify your arcpath listings in file boot.ini or through the bootcfg.exe utility.* Do not modify the boot.ini file. This message does not apply to your ftServer system.

9. When the disk is 100% resynchronized, verify that the original system disk and the upgraded system disk are healthy, resynching, dynamic, mirrored volumes. Note that the drives are not duplexed until the resynchronization activity is complete.
10. After all resynchronization activity has finished, verify that all dynamic disks are healthy, dynamic, mirrored volumes.
11. Start all applications to verify that your system and applications are working properly.

Windows Hotfixes Distributed by Stratus

To create a file that lists the Windows hotfixes distributed with your ftSSS release and that are installed on your system by an IPL or upgrade to the release, use the following procedure.

To obtain a list of Windows hotfixes

1. Insert your ftSSS for the Windows operating system DVD into the DVD drive.
2. If the ftSSS installation wizard runs automatically and asks if you want to install ftSSS, click **Cancel**.
3. In a command-prompt window, change to a directory in which to save the file.
4. Enter a command in the following format:

   dir *dvddrive*:**\Bin\Hotfix***LG*** > *outputfile*

   In the command format:

   - *dvddrive* is the drive letter for your DVD drive
   - On Windows Server 2003 systems, *LG* is the language code for your Windows version.
   - Windows Server 2008 systems do not have language versions of hotfixes; there is only one type of hotfix, regardless of the language. In the sample Windows Server 2008 system command line (below), the *kb* is the prefix that marks hotfix identifiers.

- *outputfile* is the name of the file to hold the results. You can specify any name for the file.

A sample Windows Server 2003 system command line follows:

dir D:\Bin\Hotfix*EN* > hotfixlist.txt

A sample Windows Server 2008 system command line follows:

dir D:\bin\hotfix*kb* > hotfixlist.txt

5. Eject the DVD drive.

Adaptec SAS Controller BIOS RAID Option

On an ftServer 2600, 4500, and 6300, enabling the RAID option in the Adaptec SAS controller's BIOS can make your system unbootable. If you have already encountered this problem, contact the Stratus Customer Assistance Center (CAC) or your authorized Stratus service representative for assistance.

Tape Drives and Backup on Windows Server 2008 Systems

The Windows Server 2008 built-in backup program, Windows Server Backup, does not support directly attached tape drives. To back up an ftServer Windows Server 2008 system to tape, use Symantec Backup Exec 12.5 for Windows Servers.

If you install Symantec Backup Exec 12.5 for Windows Servers, during the installation, select the **Do not use Symantec device drivers** option. Use Microsoft drivers for the tape devices instead.

Appendix A
Advanced Topics

This appendix presents the following advanced topics:

- "Using Windows Headless Mode and Console Redirection" on page A-1
- "Enabling Multiple Login Sessions (Windows Server 2008)" on page A-2

These procedures require that you change settings in the BIOS. For further information about BIOS settings, see the *Stratus ftServer Systems: Technical Reference Guide* (R550).

Using Windows Headless Mode and Console Redirection

In *headless* mode, Windows Server 2003 and 2008 systems can run without a keyboard, mouse, and monitor. You can remotely manage and restart the system through a serial connection.

NOTE

The Remote Desktop **Restrict each user to a single session setting** is set to **Yes** by default. To enable multiple simultaneous logins for a single username/account, you must disable this setting, as described in "Enabling Multiple Login Sessions (Windows Server 2008)" on page A-2.

Windows Server 2008 enables Windows Firewall but not Remote Desktop or the Firewall exception for Remote Desktop by default. You should enable Remote Desktop and the Firewall exception for Remote Desktop on your system before configuring the BIOS, as explained below.

If your system is operating in headless mode, and if the port for both console redirection and Windows headless is set to use the same serial port, configure the BIOS to stop console redirection when the power-on self-test (POST) has finished processing.

To configure the BIOS to stop console redirection after POST

1. When the system is booting and `Initializing..\` appears on the screen, begin pressing **F2** to enter the ftServer Setup utility. Wait for the BIOS setup program to run.
2. Use the RIGHT ARROW key to select the **Server** tab.
3. On the **Server** menu, use the DOWN ARROW key to select **Console Redirection**. Press **ENTER**.
4. On the **Console Redirection** menu, use the DOWN ARROW key to select **Continue C.R. after POST**. Use the PLUS SIGN key (+) to change the value to **OFF**.
5. Press **F10**.
6. In the **Setup Confirmation** dialog box, select **Yes** and press **ENTER** to save the new settings and exit from the BIOS Setup program.

Enabling Multiple Login Sessions (Windows Server 2008)

By default, Windows Server 2008 systems are set to allow only one login session for each user account.

To enable multiple login sessions

1. Click **Start**, **Administrative Tools**, **Terminal Services**, and **Terminal Services Configuration**. The Terminal Services Configuration snap-in is displayed.
2. Under **Edit Settings**, double-click **Restrict each user to a single session**.
3. Clear the check box next to **Restrict each user to a single session**.
4. Click **OK** to save and apply the change.

Modifying this setting changes the number of login sessions available to all users of the system (not only the current user account) up to the maximum available for your Windows license.

Appendix B
Configuring And Managing Ethernet PCI Adapters

You configure and manage Ethernet PCI adapters by using the Intel PROSet® utility (which the Intel Web site may refer to as Advanced Networking Software). You access PROSet from within Windows Device Manager. Using PROSet, you perform the following tasks:

- Configure Ethernet PCI adapters into teams (see "Fault-Tolerant Ethernet Teams and IP Multicasting" on page B-3 and "Configuring Ethernet Teams" on page B-5).
- Locate a PCI adapter (see "Locating Ethernet PCI Adapters" on page B-6) in a system with many Ethernet PCI adapters.
- Configure the line speed and/or duplex mode of an Ethernet PCI adapter with values appropriate to the adapter and the media to which it connects (see "Configuring Link Speed and Duplex Mode" on page B-7).
- Assign virtual LANs to a team (see "Virtual LANs" on page B-4). For information about how to configure the VLANs, see "Configuring Virtual LANs Over a Team" on page B-14.
- Manage a team by removing or adding adapters, or removing the team (see "Managing Ethernet Teams" on page B-21).
- Modify the advanced settings of an individual Ethernet PCI adapter, a team, or a VLAN.
- Troubleshoot Ethernet PCI adapters (see "Using Diagnostics" on page B-29).
- Rename an incorrectly named Ethernet team (see "Renaming Ethernet Teams" on page B-31).

NOTES

1. In systems with more than one enclosure, you can physically remove an enclosure without disrupting the network **only if the active Ethernet PCI adapters in the enclosure are teamed with adapters in another enclosure**. Note that with Adaptive Load Balancing and Link Aggregation teams, your system will

experience a drop in throughput while the enclosure is absent.

2. For fault tolerance, configure your Ethernet PCI adapters into teams. Although ftServer systems support unteamed Ethernet PCI adapters, an unteamed Ethernet PCI adapter is a single point of failure that can cause the loss of a network connection.
3. After you finish each configuration procedure, click **OK** in the dialog box to preserve your changes. If you do not click **OK** before exiting the dialog box, the configuration procedure is incomplete, and you will have to repeat it.

Using Device Manager to Manage Ethernet Adapters

You use Windows Device Manager to configure and manage Ethernet adapters and adapter teams on ftServer systems. Windows Device Manager interacts with the PROSet utility.

NOTE

To install or use ProSet functionality within Device Manager, you must be logged on with Administrator permissions.

To use Device Manager to manage Ethernet adapters

1. Go to Computer Management and then **Device Manager**.
2. In Device Manager, expand **Network adapters** to select an individual adapter or adapter team to configure or manage.

Fixing Duplicate Network Adapter Names

On Windows Server 2008 systems, duplicate Network Adapter names may appear in Device Manager after an initial program load (IPL) or when adding PCI Ethernet Adapter cards. The duplicated names will cause incorrect reporting of network information, in which case, teamed adapters will not be duplexed.

To fix duplicate network adapter names

1. Remove any teams that contain adapters with duplicate names, and uninstall the adapters with the duplicate names.

2. Use the **Scan for hardware changes** command to reconfigure the network adapters with unique names. To use **Scan for hardware changes**:
   a. Go to Computer Management and then **Device Manager**.
   b. In Device Manager, expand **Network adapters**.
   c. Right-click the target adapter and select **Scan for hardware changes**.
3. Create any required teams again.

Use Windows Remote Desktop if you need to start Device Manager remotely. You can then create or modify a team if it is not carrying your connection to the system.

NOTE

Do not modify the team that provides your connection to the system. Doing so will result in a loss of network connection.

Online help appears automatically as you use Device Manager to configure and manage Ethernet adapters.

Fault-Tolerant Ethernet Teams and IP Multicasting

If IP multicasting is in use on your network, consider the following restriction when choosing the type of fault-tolerant team to configure.

For an overview of the supported types of teams, see the online “ANS Teaming Overview” that is within Device Manager.

To see the ANS teaming overview on a Windows Server 2008 system

1. In the Network adapters node in Device Manager, right-click a target adapter and select **Properties**.
2. Click the **Teaming** tab.
3. In the bottom panel of the dialog box, click the **click here** link.

To access the ANS teaming overview on a Windows Server 2003 system

1. In the Network adapters node in Device Manager, right-click the target adapter and select **Properties**.
2. Click the **Teaming** tab on the Properties dialog box.
3. Under Teaming options, choose the **Team this with other adapters** button.
4. In the bottom panel of the same dialog box, click the **ANS Teaming Overview** link.
5. Click the **ANS Team Types** link for a description of the supported team types.

Each network host in an IP multicast group uses the Internet Group Management Protocol (IGMP) to acknowledge and maintain its IP multicast group membership with a switch.

In an Adapter Fault Tolerance (AFT), Switch Fault Tolerance (SFT), or Adaptive Load Balancing (ALB) team, only one Ethernet PCI adapter (the primary adapter) is registered to receive IP multicast packets. When failover to another adapter occurs, the host cannot automatically update its multicast group membership using the new primary adapter; therefore, the host stops receiving multicast packets. If the switch is configured to periodically query the host for its registration, or if static IGMP is configured on the switch for each adapter in the team, multicasting to the host will eventually resume, but possibly after an extended interruption.

If you use IP multicasting, and you want to configure an AFT, SFT, or ALB team, you should test the team on site to verify if the behavior of IP multicasting after failover is acceptable. Alternatively, you can configure either static or dynamic link aggregation teams. IP multicasting functions more reliably with qualified switches that support these modes, because all Ethernet PCI adapters in a link aggregation team are registered to receive the IP multicast packets. The team continues to receive IP multicast packets unless all links to the switch are lost and then restored (in which case, there is also an extended interruption).

For more information about IP multicasting, see the documentation for your switch, or contact your network administrator.

Virtual LANs

You can add a Virtual LAN (VLAN) to any type of Ethernet team.

NOTE

Stratus supports VLANs only over Ethernet teams, not over individual adapters. An unteamed adapter is a single point of failure that can cause the loss of a network connection.

A VLAN allows you to isolate network traffic for a specific group of network hosts. Using VLANs, you can organize networked systems into logical workgroups, such as Marketing or Engineering, that span a building, complex, or an entire enterprise network. Members of a particular VLAN receive traffic only from other members of the same VLAN.

VLANs are particularly useful for limiting broadcast storms, reducing security problems, and simplifying network management.

There are two types of VLANs:

- Implicit VLANs, which are configured entirely at the switch level. The switch does not alter or tag packets to enforce an implicit VLAN.
- Explicit VLANs, which are configured throughout the network, on each adapter and link partner. Switches identify and route traffic based on a four-byte tag (802.3ac) in each packet header.

To support either type of VLAN, switches on your network must support 802.1Q VLANs. Also, to configure a VLAN on your system, you need to contact your network administrator to obtain the VLAN ID for your workgroup, which must be identical to the VLAN ID programmed into the switches.

In an environment with many VLAN workgroups, you can optionally implement the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) to dynamically create, change, and remove VLANs. To support GVRP, all adapters and switches on your network must have GVRP enabled. For more information about GVRP, follow the links in the online help available on the VLANs tab and the documentation for your switch, or contact your network administrator.

Configuring Ethernet Teams

Use the utilities embedded in Device Manager to configure Ethernet PCI adapters into teams. Keep the following notes, guidelines, and restrictions in mind when you create a team.

- Each port on a dual-port Ethernet PCI adapter appears as a separate adapter in the **Network adapters** node of Device Manager.
- Generally, assign Ethernet PCI adapters of only one media type (fiber optic or copper) to a team.
- By default, speed and duplex are autonegotiated. Autonegotiation will result in incorrect duplex settings if one side of the link is set to autonegotiate and the other side of the link is not. Always confirm how the switch ports that will be connected to the network ports on the server are configured, and configure the network ports on the server the same way. Always use the same data rate and duplex mode values for all members of a team
- There is no minimum or maximum number of teams to be configured; teams are limited only by the number of adapters available on your system and how you allocate them.
- One team can have a maximum of eight Ethernet PCI adapters.
- For fault tolerance, create teams that contain Ethernet PCI adapters from different I/O elements. Only teams with Ethernet PCI adapters in different I/O elements are

fault tolerant. (See “Locating Ethernet PCI Adapters” on page B-6 for information about locating Ethernet PCI adapters.)

In addition, Stratus does not support the following:

- Manipulation of adapter power management options.
- Teaming third-party Ethernet PCI adapters with Stratus Ethernet PCI adapters. Only Stratus Ethernet PCI adapters have been tested for compatibility and fault tolerance in ftServer systems.

To configure Ethernet PCI adapters into fault-tolerant teams, perform the procedures described in the following sections, in the order listed.

1. “Locating Ethernet PCI Adapters” on page B-6
2. “Configuring Link Speed and Duplex Mode” on page B-7
3. “Creating Ethernet Teams” on page B-10
4. “Configuring Virtual LANs Over a Team” on page B-14
5. “Verifying the Configuration of Teams and VLANs” on page B-16
6. “Assigning an IP Address to a Team or VLAN” on page B-18

Locating Ethernet PCI Adapters

When you create a team of Ethernet PCI adapters, you must connect the team members to adapters located in different I/O elements or the team will not be fault-tolerant, since the failure of the team’s I/O element will cause both team members to fail.

To help you verify that you are selecting adapters located in different I/O elements, use the Identify Adapter command to flash a status LED in a specific Ethernet port so you can visually locate it.

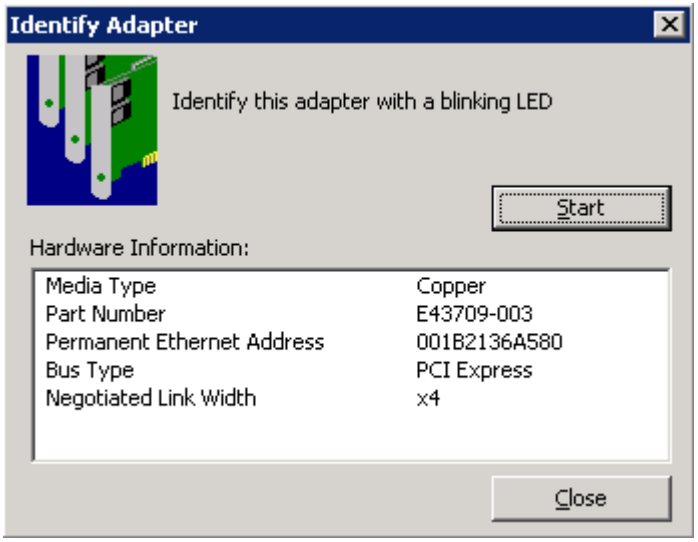
NOTE

To determine which LED on the Ethernet port will flash, see the *Stratus ftServer Systems: PCI Adapter Guide* (R461).

To locate an Ethernet PCI adapter port

1. In the Network adapters node in Device Manager, right-click the target adapter and select **Properties**.
2. Click the **Link Speed** tab and then **Identify Adapter**. The **Identify Adapter** dialog box appears. Figure B-1 shows an example.

Figure B-1. Identify Adapter Dialog Box



3. On the Identify Adapter dialog box, click **Start**.

   The LED on the selected adapter will flash until you click **Stop** on the Identify Adapter dialog box.

4. Find the Ethernet port with the flashing LED and make note of its device name in Device Manager (for example, Stratus 82576 2-port Copper Gigabit Adapter).
5. When you have identified the adapter, click **Stop** and then **Close** on the **Identify Adapter** dialog box.

Configuring Link Speed and Duplex Mode

By default, Ethernet ports on the U104 Dual-Port Fiber Gigabit Ethernet PCI-Express Adapter, the U105 Dual-Port 10/100/1000 Base-T Ethernet PCI-Express Adapter, and the embedded Ethernet PCI adapters are configured to autonegotiate the best speed for a connection. On a network that operates at 10 or 100 megabits per second (Mbps), automatic settings can result in unreliable connections and inaccurate reporting of link activity and *duplex mode*. For reliable operation, manually configure the link speed and duplex mode for all Ethernet PCI adapters connected to networks that operate at 10 or 100 Mbps.

The term *duplex* in *duplex* mode is unrelated to the term *duplexed* used when referring to PCI adapters that are duplexed for fault-tolerance. Duplex mode refers to the ability of a communications line (which is attached to an Ethernet PCI adapter) to send and receive data simultaneously. In full-duplex mode, the line can send and receive data simultaneously. In half-duplex mode, the line can only send or receive data at any given

moment. Duplex mode does not refer to whether or not a PCI adapter is one of a pair, or is teamed, for fault-tolerance.

NOTES

1. Ethernet adapters or ports that are connected to networks running at one gigabit per second (Gbps) rely on autonegotiation. Do not manually configure 1-Gbps operation.
2. ftServer systems support 1-Gbps line speed only in full-duplex mode.

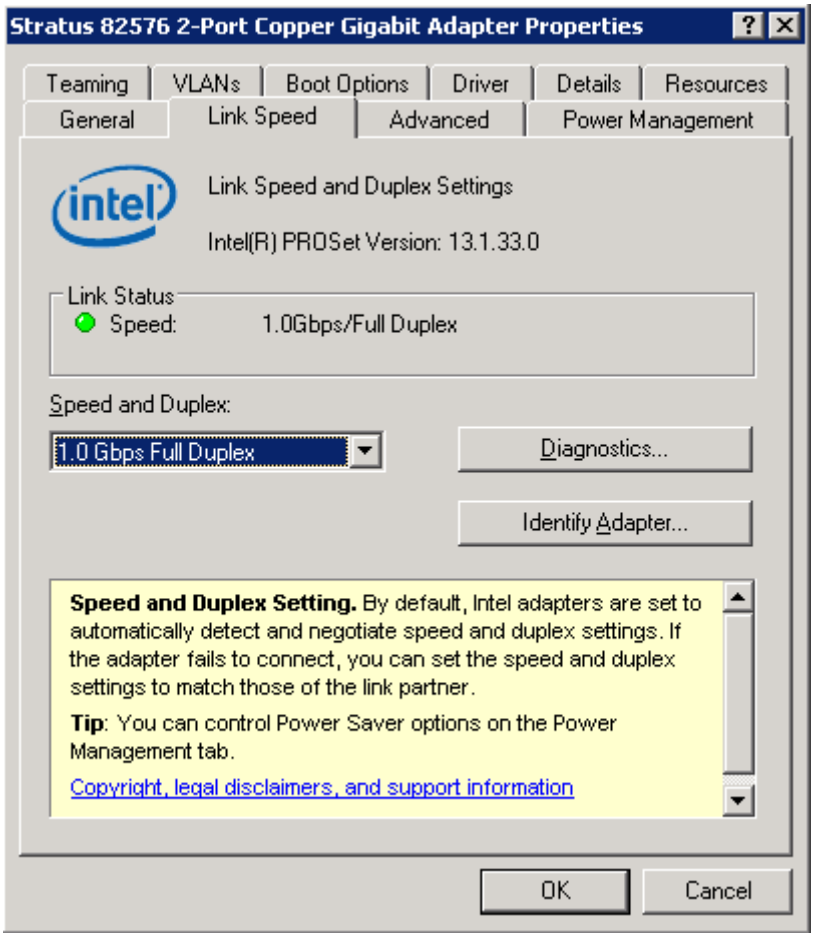
CAUTION

When you manually set these values, make sure that the values are identical for the Ethernet port and the link partner to which it connects, and that the settings for all Ethernet ports in one team are the same.

To set the link speed and duplex mode

1. In the Network adapters node in Device Manager, right-click the target adapter (if necessary, expand a team to access its member adapters) and select **Properties**.
2. Click the **Link Speed** tab.
3. In the **Speed and Duplex** section of the dialog box, select the appropriate speed and duplex mode from the pull-down menu. Figure B-2 shows an example.

Figure B-2. Setting the Link Speed and Duplex Mode


Stratus 82576 2-Port Copper Gigabit Adapter Properties
Teaming
VLANs
Boot Options
Driver
Details
Resources
General
Link Speed
Advanced
Power Management
Link Speed and Duplex Settings
Intel(R) PROSet Version: 13.1.33.0
Link Status
Speed:
1.0Gbps/Full Duplex
Speed and Duplex:
1.0 Gbps Full Duplex
Diagnostics...
Identify Adapter...
Speed and Duplex Setting. By default, Intel adapters are set to automatically detect and negotiate speed and duplex settings. If the adapter fails to connect, you can set the speed and duplex settings to match those of the link partner.
Tip: You can control Power Saver options on the Power Management tab.
Copyright, legal disclaimers, and support information
OK
Cancel

4. Repeat the previous two steps for each Ethernet PCI adapter for which you need to set the link speed and duplex mode.
5. Click **OK** to process and preserve the changes. Allow several seconds for processing time.
6. Click **OK** to exit.

Creating Ethernet Teams

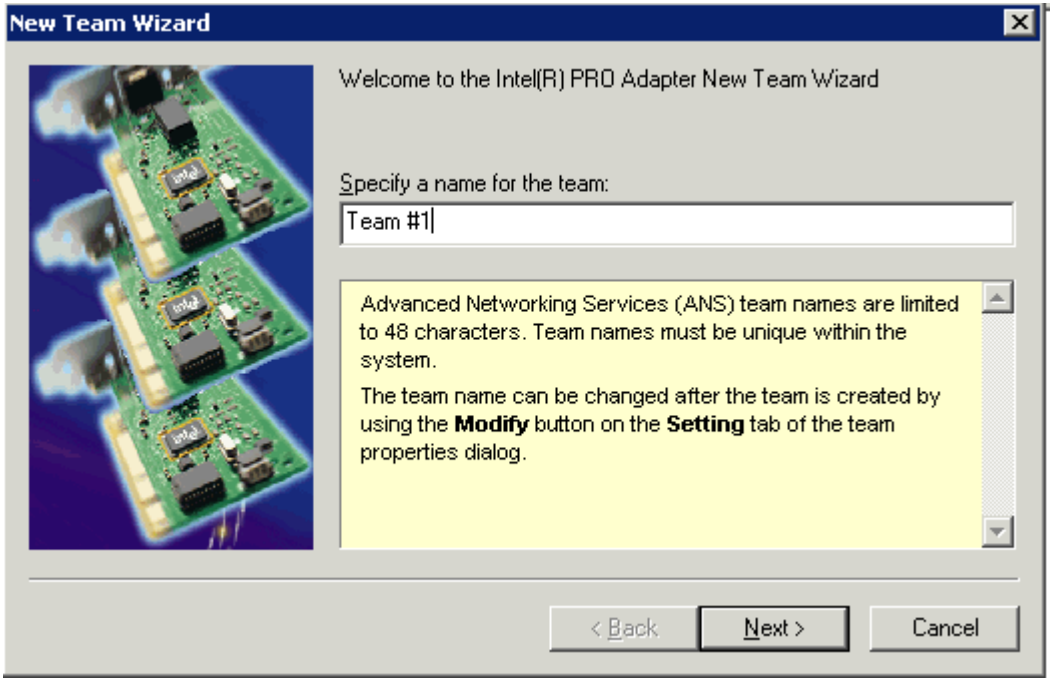
CAUTION

Creating an Ethernet team disrupts the network traffic over all Ethernet PCI adapters in the team.

To create an Ethernet team

1. In the Network adapters node in Device Manager, right-click the adapter that you want to team with another adapter, and select **Properties**.
2. On the **Teaming** tab, select **Team this adapter with other adapters**.
3. Click **New Team**. The **New Team Wizard** starts.
4. In the New Team Wizard dialog box, specify a team name under **Specify a name for the team**. Figure B-3 shows an example. Online Help, which appears in the yellow panel at the bottom of the dialog box, automatically explains the requirements of the team name. Click **Next**.

Figure B-3. Naming the New Team


New Team Wizard
Welcome to the Intel(R) PRO Adapter New Team Wizard
Specify a name for the team:
Team #1
Advanced Networking Services (ANS) team names are limited to 48 characters. Team names must be unique within the system.
The team name can be changed after the team is created by using the Modify button on the Setting tab of the team properties dialog.
< Back
Next >
Cancel

5. The next dialog box lists the adapters and displays a check in the box next to the adapter you selected in step 1. Under **Select the adapters to include in this**

team, check the box next to the adapter you want to team with the adapter you selected in step 1.

As you select adapters for a team, follow the notes, guidelines, and restrictions listed at the beginning of this section ("Configuring Ethernet Teams" on page B-5).

Click **Next**.

6. In the next dialog box, under **Select a team type**, select the type of team you want to create (for example, **Adapter Fault Tolerance**), and then click **Next**.

   Online Help provides a description of the types of teams you can create.

7. A dialog box reports that the application has the settings it needs to create the team. Depending on the teaming mode you select, the dialog box may also display information about the restrictions for the specified teaming mode.

   Click **Finish**.

If you created an ALB team, you must disable the Receive Load Balancing setting, as explained in the next section.

The PROSet utility begins to bind the specified PCI adapters into teams. This operation takes at least one minute per team to complete. **Do not abort** the process while it is running; otherwise, you must repeat the procedure.

After several seconds, the team is created and the Team Properties page appears.

Disabling Receive Load Balancing

If you created an ALB team, you must disable the Receive Load Balancing setting after you have created the ALB team.

NOTE

If you do not disable Receive Load Balancing, the I/O enclosures are not safe to pull.

To disable Receive Load Balancing

1. In the Network adapters node in Device Manager, right-click the ALB team you just created and select **Properties**.
2. Click on the **Advanced** tab and select **Receive Load Balancing** in the Settings list. It is enabled by default.
3. In the value box, change Enabled to **Disabled** and click **OK**.

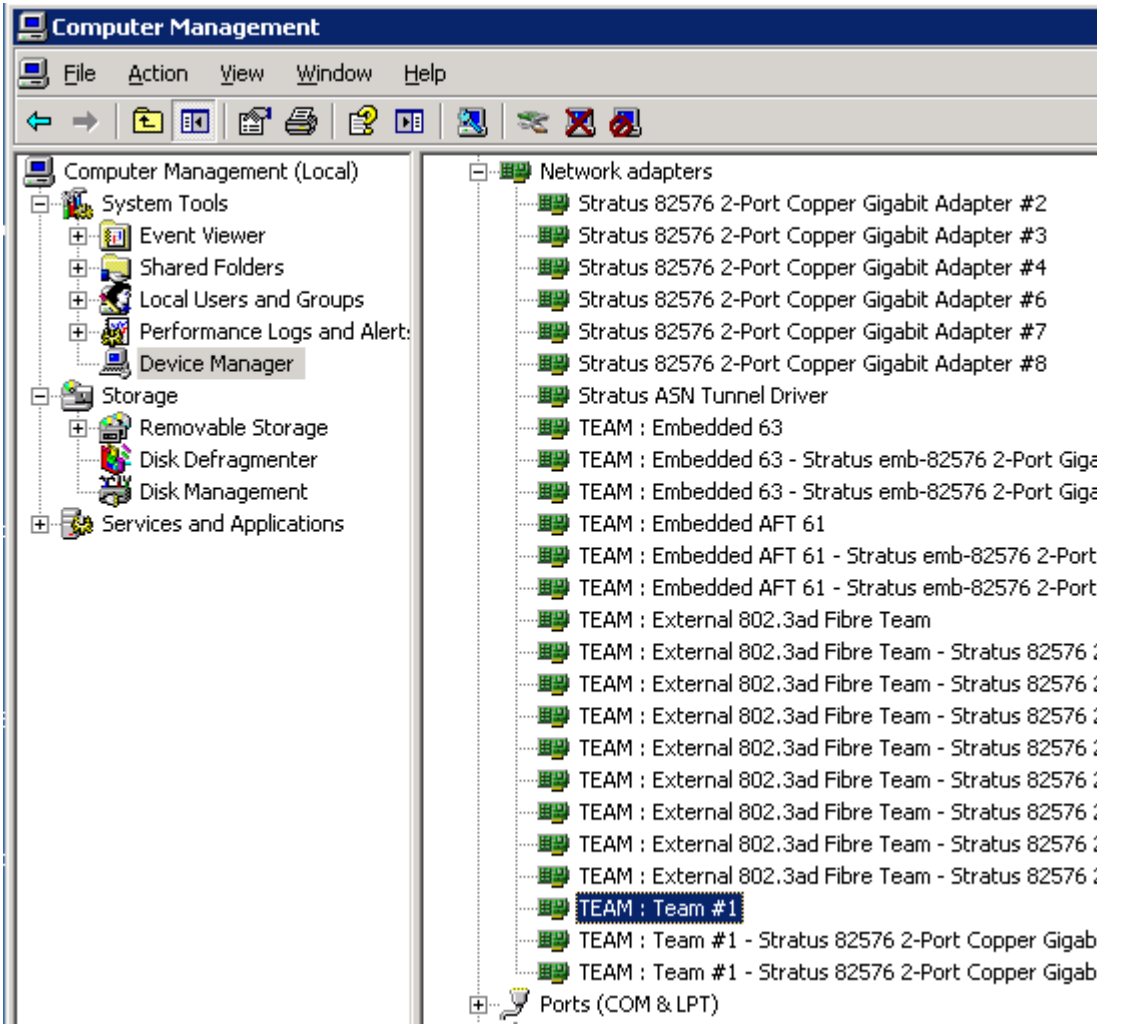
Designating Primary and Secondary Adapters

After creating the teams, you can manually designate a primary and secondary adapter for each team.

To designate primary and secondary adapters

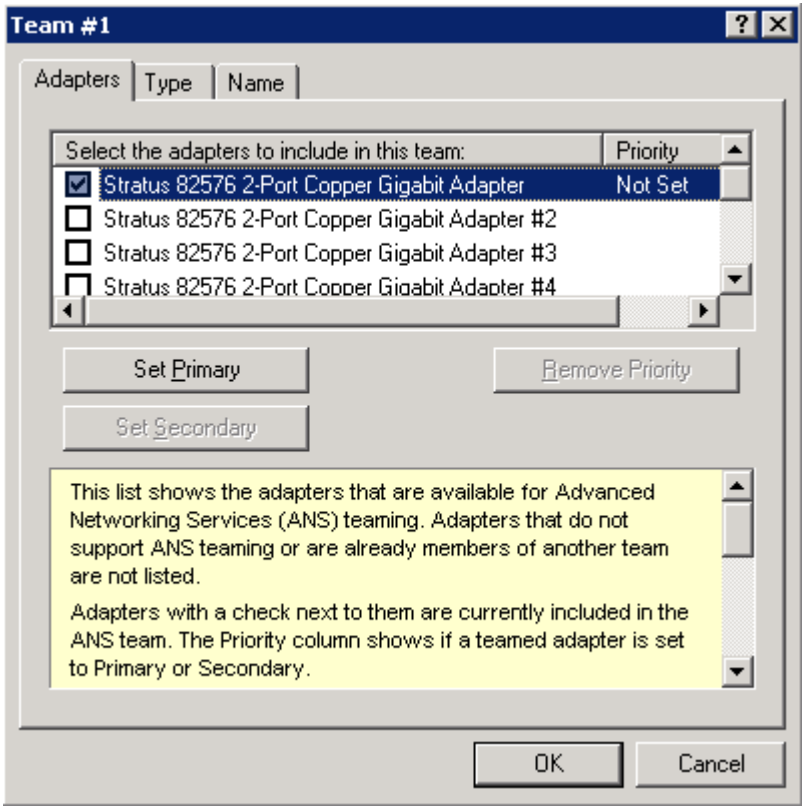
1. In the Network adapters node in Device Manager, right-click the team (not the adapter; see Figure B-4) in which you want to designate a primary and (optionally) a secondary adapter, and select **Properties**.

Figure B-4. Network Adapters in Device Manager


Computer Management
File
Action
View
Window
Help
Computer Management (Local)
System Tools
Event Viewer
Shared Folders
Local Users and Groups
Performance Logs and Alert:
Device Manager
Storage
Removable Storage
Disk Defragmenter
Disk Management
Services and Applications
Network adapters
Stratus 82576 2-Port Copper Gigabit Adapter #2
Stratus 82576 2-Port Copper Gigabit Adapter #3
Stratus 82576 2-Port Copper Gigabit Adapter #4
Stratus 82576 2-Port Copper Gigabit Adapter #6
Stratus 82576 2-Port Copper Gigabit Adapter #7
Stratus 82576 2-Port Copper Gigabit Adapter #8
Stratus ASN Tunnel Driver
TEAM : Embedded 63
TEAM : Embedded 63 - Stratus emb-82576 2-Port Giga
TEAM : Embedded 63 - Stratus emb-82576 2-Port Giga
TEAM : Embedded AFT 61
TEAM : Embedded AFT 61 - Stratus emb-82576 2-Port
TEAM : Embedded AFT 61 - Stratus emb-82576 2-Port
TEAM : External 802.3ad Fibre Team
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : External 802.3ad Fibre Team - Stratus 82576
TEAM : Team #1
TEAM : Team #1 - Stratus 82576 2-Port Copper Gigab
TEAM : Team #1 - Stratus 82576 2-Port Copper Gigab
Ports (COM & LPT)

2. Select the **Settings** tab and click **Modify Team**.
3. In the Team dialog box, select the adapter to make primary, click **Set Primary**, and click **OK**. Figure B-5 shows an example. (Click **Set Secondary** on an adapter to make it the secondary adapter.)

Figure B-5. Assigning Priorities to Ethernet PCI Adapters


Team #1
Adapters
Type
Name
Select the adapters to include in this team:
Priority
Stratus 82576 2-Port Copper Gigabit Adapter
Not Set
Stratus 82576 2-Port Copper Gigabit Adapter #2
Stratus 82576 2-Port Copper Gigabit Adapter #3
Stratus 82576 2-Port Copper Gigabit Adapter #4
Set Primary
Remove Priority
Set Secondary
This list shows the adapters that are available for Advanced Networking Services (ANS) teaming. Adapters that do not support ANS teaming or are already members of another team are not listed.
Adapters with a check next to them are currently included in the ANS team. The Priority column shows if a teamed adapter is set to Primary or Secondary.
OK
Cancel

NOTE

You can select only one primary adapter and only one secondary adapter per team. If you select another primary or secondary adapter, it overrides your initial selection.

In the Team Properties dialog box, click **OK**.

4. To confirm your selections, in Device Manager, right-click the team (for example, TEAM: Team #0, select **Properties**, and select the **Settings** tab to see the Primary or Secondary indications next to the listed adapters.

Configuring Virtual LANs Over a Team

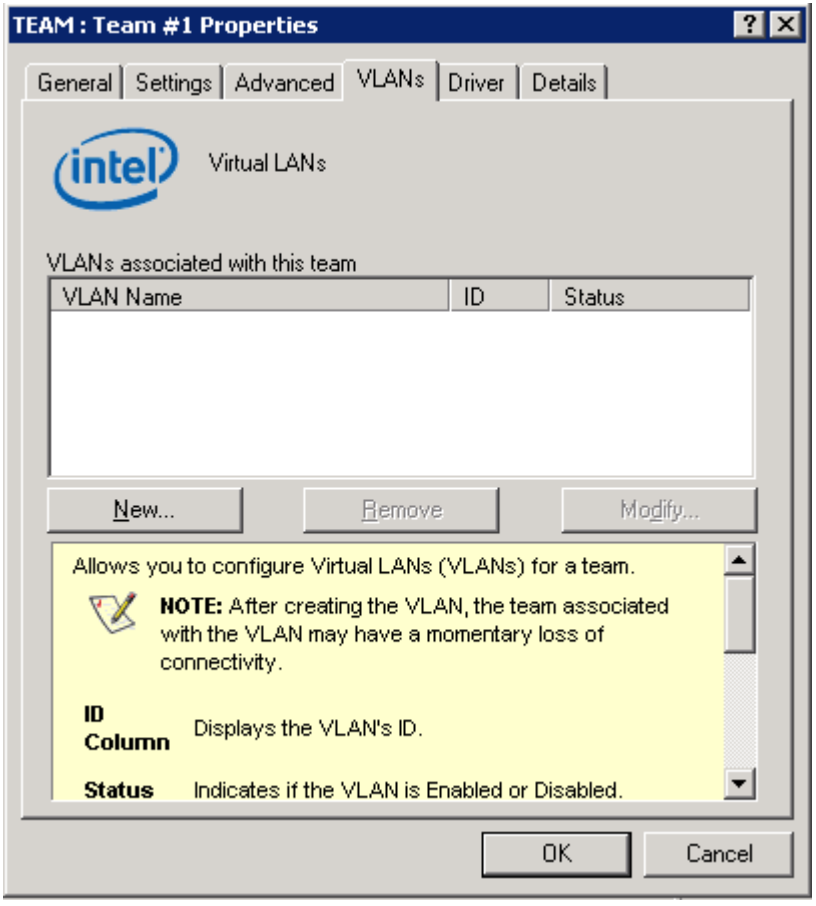
Configuring VLANs is optional. You can have an Ethernet team without VLANs.

CAUTION

Configuring a VLAN over an Ethernet team disrupts the network traffic over the team.

1. In the Network adapters node in Device Manager, right-click the targeted adapter **team** and select **Properties**.
2. Select the **VLANs** tab. See Figure B-6.

Figure B-6. Adding a VLAN to a Team

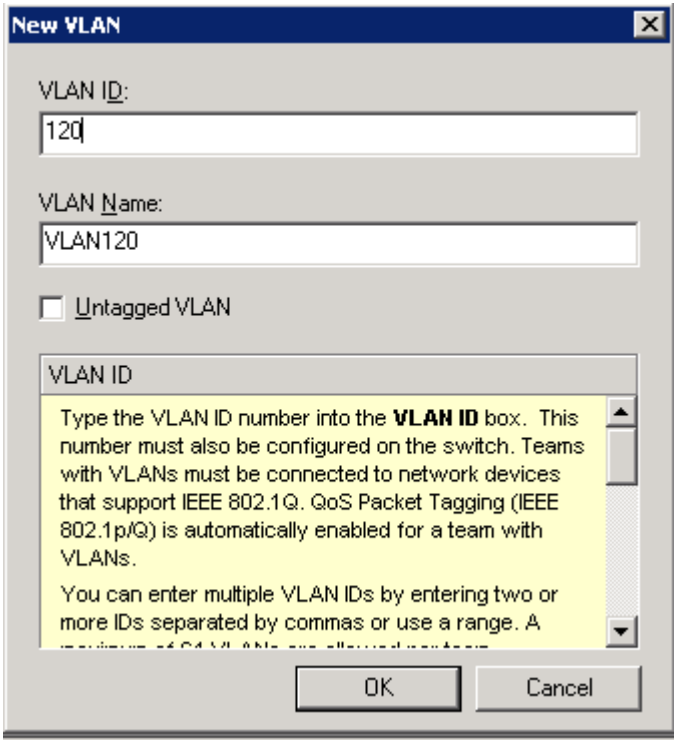


3. On the **VLANs** tab, click **New**.

4. In the **New VLAN** dialog box, enter the VLAN ID. Figure B-7 shows an example. The VLAN ID must match the VLAN ID configured on the switch.

   As you enter the VLAN ID, the ID appears in the VLAN Name field, preceded by the suffix VLAN. For example, if you enter **120** in the VLAN ID field, the name **VLAN120** appears automatically in the VLAN Name field.

Figure B-7. Specifying a VLAN ID and Name


New VLAN
VLAN ID:
120
VLAN Name:
VLAN120
Untagged VLAN
VLAN ID
Type the VLAN ID number into the VLAN ID box. This number must also be configured on the switch. Teams with VLANs must be connected to network devices that support IEEE 802.1Q. QoS Packet Tagging (IEEE 802.1p/Q) is automatically enabled for a team with VLANs.
You can enter multiple VLAN IDs by entering two or more IDs separated by commas or use a range. A
OK
Cancel

5. Click **OK**. The new entry for the VLAN appears in Device Manager under the **Network adapters** node.

   You can create up to 64 VLANs on a system.

Verifying the Configuration of Teams and VLANs

1. Close and then restart Device Manager. In Device manager, verify the following:
   - The teams and VLANs have been created as you expected.
   - All Ethernet PCI adapters in a team use the same Ethernet address, and that address is the permanent Ethernet address of one of the Ethernet PCI adapters in the team. (See "Updating a Team's Ethernet Address" on page B-25 for more information.

2. Verify that an IP address has been assigned to each team or VLAN.

   If you have created a team with VLANs, each VLAN in that team requires an IP address. (The team and the Ethernet PCI adapters in the team have no IP addresses.)

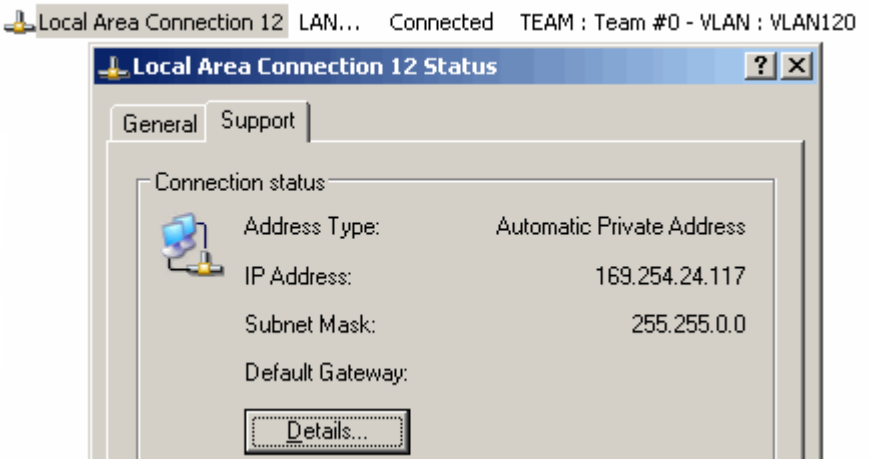
   If you created a team without VLANs, the team is configured to obtain an IP address automatically.

   If a team requires a static IP address, or if a team or VLAN does not have an IP address, configure the IP address as described in "Assigning an IP Address to a Team or VLAN" on page B-18. (Individual Ethernet PCI adapters in a team do not have IP addresses.)

   Find the IP address for a team with or without VLANs, as follows:

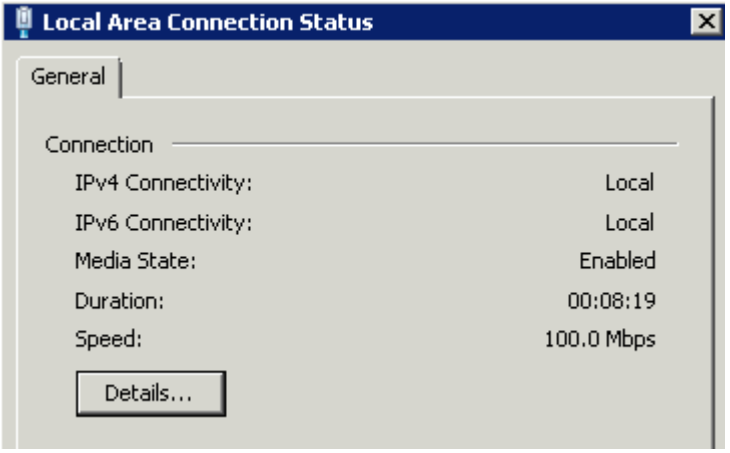
   - On a Windows Server 2003 system, click **Start**, **All Programs**, **Accessories**, **Communications**, and then **Network Connections**. Click the desired Local Area Connection icon for the VLAN or team (for example, Team #0, as shown in Figure B-8), and click the **Support** tab on the dialog box to see the IP address.

Figure B-8. Finding a Team's IP Address in Windows 2003



- On a Windows Server 2008 system, click **Start**, **Control Panel**, and then **Network And Sharing Center**. Listed under **Network** and **Connections**, find the desired Local Area Connection for the VLAN or team, and click **View Status.** In the dialog box that appears, click **Details**, as shown in Figure B-9.

Figure B-9. Finding a Team's IP Address in Windows 2008



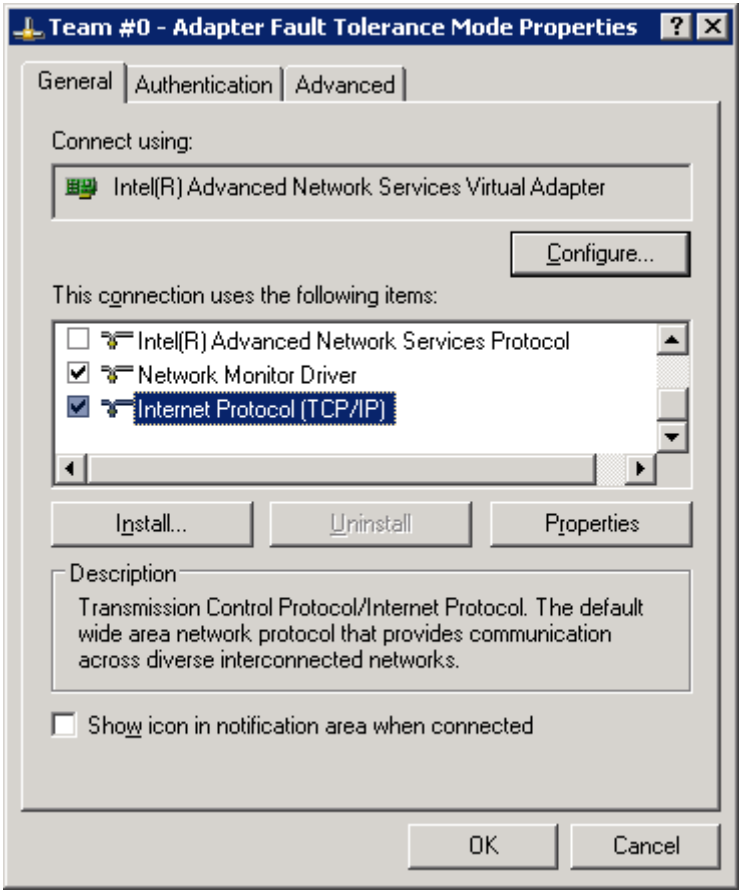
In the Details window that appears, the IP address is listed as **IPv4 IP Address**.

3. Start ftSMC, select each **Network Port** you teamed, and in the details pane, verify that the value next to **OpState: State** is **Duplexed**.

Assigning an IP Address to a Team or VLAN

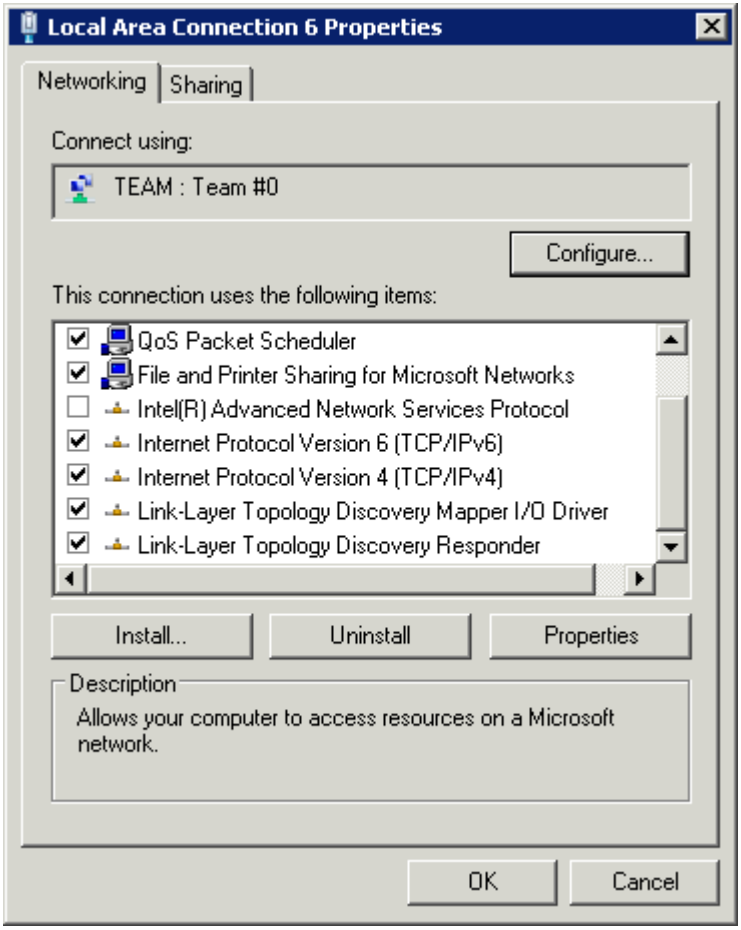
1. Perform one of the following steps to start to manage network connections.
   - On a Windows Server 2008 system, click **Start**, **Control Panel**, **Network and Sharing Center**, and then **Manage Network Connections**.
   - On a Windows Server 2003 system, click **Start**, **All Programs**, **Accessories**, **Communications**, and then **Network Connections**.
2. In the window that appears, right-click the appropriate **Team #*n*** or **VLAN *Name*, ID: *n*** icon, and then click **Properties**.
3. In the **Properties** dialog box that appears, perform the following steps:
   - On a Windows Server 2003 system, click **Internet Protocol (TCP/IP)**, and click **Properties**. Figure B-10 shows an example.

Figure B-10. Ethernet Team Properties on a Windows Server 2003 System



- On a Windows Server 2008 system, click either **Internet Protocol Version 6 (TCP/IPv6)** or **Internet Protocol Version 6 (TCP/IPv6)**. Figure B-11 shows an example.

Figure B-11. Ethernet Team Properties on a Windows Server 2003 System

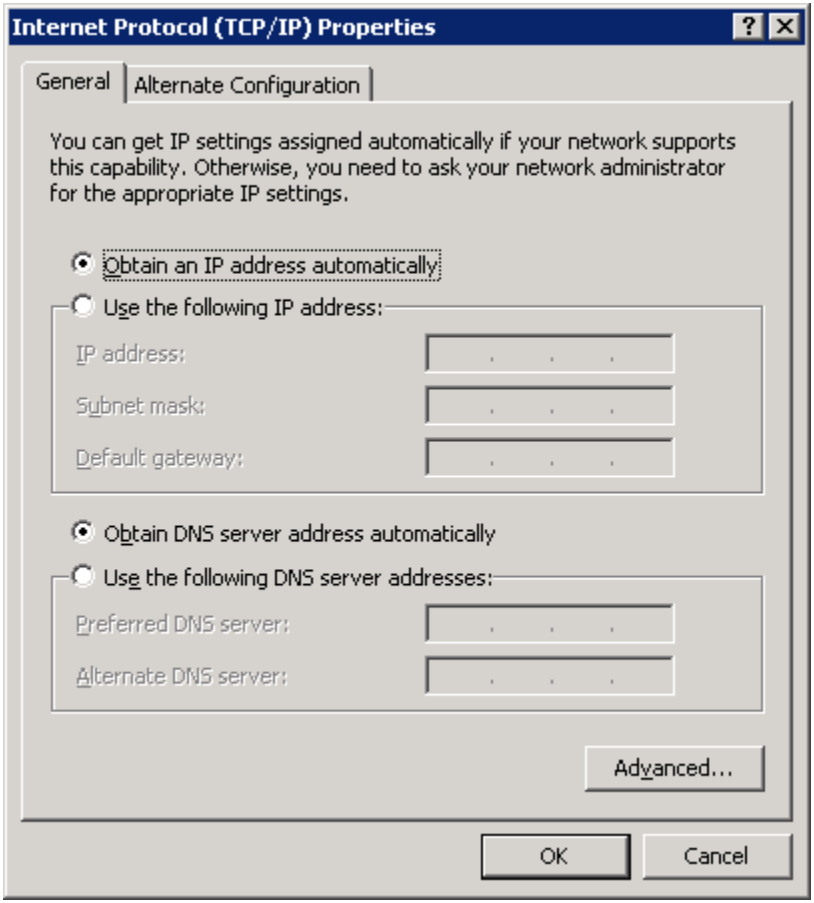


In the **Properties** dialog box on a Windows Server 2003 or 2008 system, select whether you want to specify an IP address or to obtain the IP address automatically. Figure B-12 shows the dialog box for a Windows Server 2003 system. If you specify an IP address, enter the IP address, subnet mask, and default gateway. Consult your network administrator for all TCP/IP property settings.

NOTE

Your TCP/IP property settings must match the configuration of the network to which the team or VLAN is connected. Your system can obtain the IP address automatically only if the network supports it. If you choose the option to obtain the IP address automatically and the network does not support it, the Ethernet PCI adapter may be unusable.

Figure B-12. Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

4. Click **OK** to accept the changes.
5. In the **Properties** dialog box, click **Close** to process the new TCP/IP settings and to close the dialog box.

6. Return to Device Manager and verify that the new IP address appears in the **Team Configuration** tab for the team or **VLAN Configuration** tab for the VLAN.

Managing Ethernet Teams

The following sections explain how to manage teams:

- "Removing Ethernet PCI Adapters from a Team" on page B-21
- "Adding Ethernet PCI Adapters to a Team" on page B-24
- "Updating a Team's Ethernet Address" on page B-25
- "Removing an Ethernet Team" on page B-28

NOTES

1. Anytime you modify an existing team, you might temporarily interrupt the flow of network traffic to the team.
2. When you add or remove Ethernet PCI adapters in an existing Static Link Aggregation team, the link to the adapters you are adding or removing must be down; otherwise, the switch forwards traffic to the adapters before the configuration is complete.
3. When you remove or replace a teamed adapter, you might need to reset the Ethernet (MAC) address of the team as described in "Updating a Team's Ethernet Address" on page B-25. In addition, your network administrator must update any network filtering or security settings that might be based on the MAC address of the Ethernet adapter you removed.

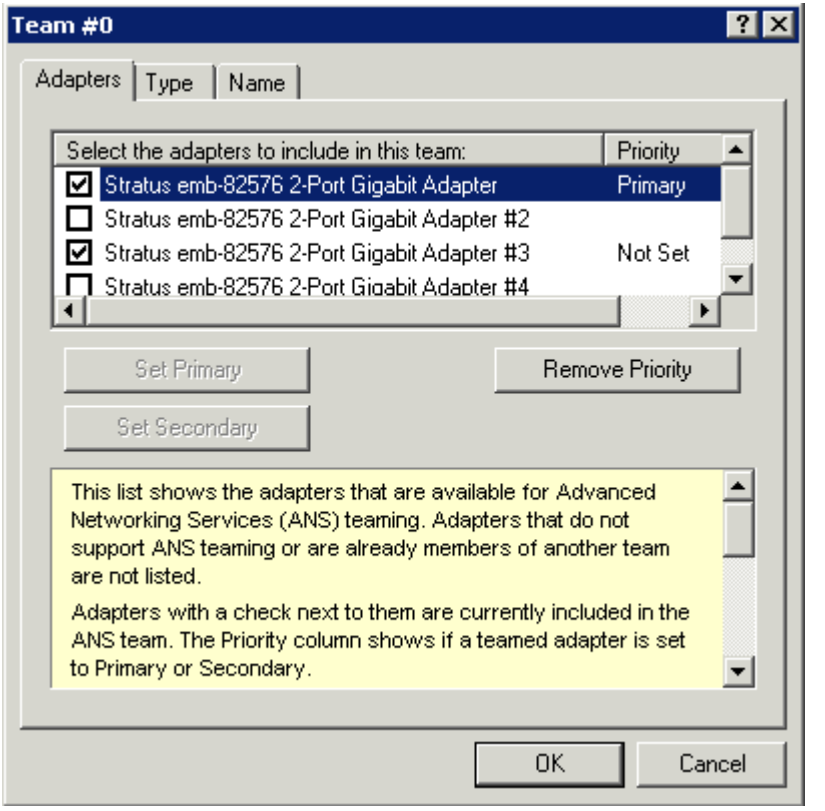
Removing Ethernet PCI Adapters from a Team

NOTE

Remove Ethernet PCI adapters from only one team at a time. Complete the procedure before removing an adapter from another team.

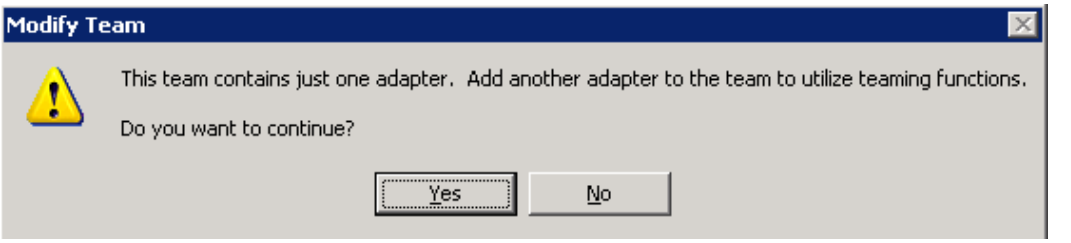
1. In the Network adapters node in Device Manager, right-click the adapter team and select **Properties**.
2. Select the **Settings** tab and click the **Modify Team** button.
3. In the Team dialog box (Figure B-13), clear the checkbox next to the adapter you want to remove from the team and click **OK**.

Figure B-13. Removing an Ethernet PCI Adapter from a Team


Team #0
Adapters
Type
Name
Select the adapters to include in this team:
Priority
Stratus emb-82576 2-Port Gigabit Adapter
Primary
Stratus emb-82576 2-Port Gigabit Adapter #2
Stratus emb-82576 2-Port Gigabit Adapter #3
Not Set
Stratus emb-82576 2-Port Gigabit Adapter #4
Set Primary
Remove Priority
Set Secondary
This list shows the adapters that are available for Advanced Networking Services (ANS) teaming. Adapters that do not support ANS teaming or are already members of another team are not listed.
Adapters with a check next to them are currently included in the ANS team. The Priority column shows if a teamed adapter is set to Primary or Secondary.
OK
Cancel

4. A confirmation message appears. If the team contained only two Ethernet PCI adapters, a dialog box warns that the team contains only one adapter, as shown in Figure B-14. Click **OK**.

Figure B-14. Confirmation Message: Removing an Ethernet PCI Adapter from a Team


Modify Team
This team contains just one adapter. Add another adapter to the team to utilize teaming functions.
Do you want to continue?
Yes
No

If desired, you can designate new primary and secondary adapters for the team as described in “Designating Primary and Secondary Adapters” on page B-12.

If you remove the primary or secondary adapter in the team, the program automatically designates other team members to fill these roles, but you can optionally assign them yourself.

If you are not physically replacing the Ethernet PCI adapters that you removed, update the Ethernet address of the team at this time. See "Updating a Team's Ethernet Address" on page B-25.

Physically Replacing Removed Adapters

If you intend to physically replace the adapters you removed, complete the following procedure.

To physically replace adapters in a team

1. If you intend to maintain network connectivity while removing an enclosure, verify that all active Ethernet PCI adapters in the enclosure are teamed with adapters in another enclosure. See "Locating Ethernet PCI Adapters" on page B-6 to determine the location of Ethernet PCI adapters in the system.
2. Exit the adapter configuration program.
3. Physically remove the Ethernet PCI adapters from the system and install the new adapters. For more information about removing and replacing adapters, see the operation and maintenance guide for your system.

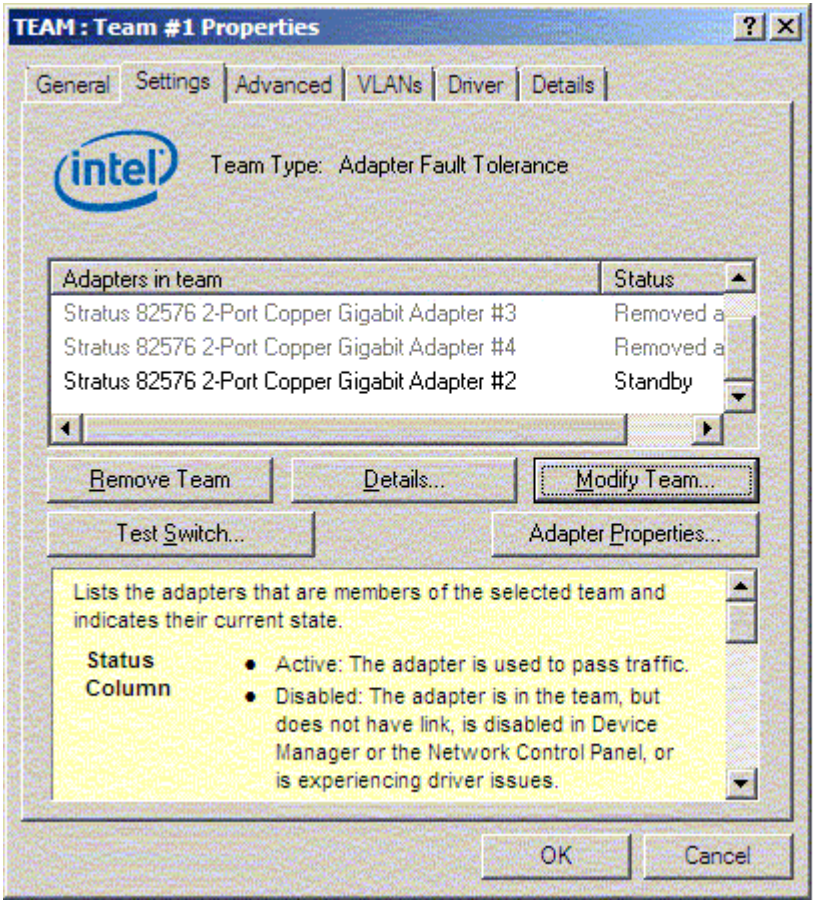
   NOTE

   If you intend to use the old Ethernet PCI adapters in other systems, do not install them in other systems until you reset the Ethernet address of the team (when you reach step 4 of "Adding Ethernet PCI Adapters to a Team").

4. In the Network adapters node in Device Manager, right-click the adapter team and select **Properties**.
5. Select the **Settings** tab and click the **Modify Team** button.
6. In the Team dialog box, clear the checkbox next to the adapter you want to remove from the team and click **OK**.
7. Remove the entries for the Ethernet PCI adapters that you physically removed from the system. The adapters have the status **Removed adapter** (Figure B-15).

   For each adapter you want to remove, right-click the adapter entry and select **Remove Adapter**. When you are finished, click **Apply** to process the changes.

Figure B-15. Icon for a Missing (Removed) Adapter



8. Add the new Ethernet PCI adapters to the team, as "Adding Ethernet PCI Adapters to a Team" describes.

Adding Ethernet PCI Adapters to a Team

NOTES

1. Add Ethernet PCI adapters to only one team at a time. Complete the procedure before adding an adapter to another team.
2. One team can have a maximum of eight Ethernet PCI adapters.

1. In the Network adapters node in Device Manager, right-click the target adapter team and select **Properties**.
2. Select the **Settings** tab, and click the **Modify Team** button.

   In the TEAM dialog box (Figure B-13), place a check in the checkbox next to the adapter you want to add to the team. Click **OK**.

   Repeat this step for any adapters you want to add to the team.

   The Settings tab appears, showing the newly added adapter team.

   Click **OK**.

   The Device Manager appears again, showing the newly configured adapter team in the Network adapters node.

3. If necessary, you can manually designate new primary and secondary adapters for the team. See "Designating Primary and Secondary Adapters" on page B-12.

   (If you have not previously selected primary or secondary adapters for the team, the utility will automatically designate adapters to fill these roles.)

4. If necessary, reset the Ethernet address of the team. See "Updating a Team's Ethernet Address" on page B-25.
5. If you have not already done so, connect the new Ethernet PCI adapters to the network.
6. Verify the configuration of the team. See "Verifying the Configuration of Teams and VLANs" on page B-16.

Updating a Team's Ethernet Address

CAUTION

When you update a team's Ethernet address, the network connection is disrupted.

When you replace a **primary** Ethernet PCI adapter, you must assign the correct Ethernet address to the team before you connect the new primary adapter to the network.

NOTE

Assigning the correct Ethernet address to the team before you connect the new primary adapter to the network applies only to Ethernet PCI adapters that you insert into

slots. It does not apply to embedded Ethernet adapters when you replace an I/O enclosure.

Typically, the team Ethernet address is the permanent MAC address of the primary adapter. When you replace a primary adapter, the team by default continues to use the MAC address of the adapter you removed. Therefore, after you replace an adapter, you must assign the team an Ethernet address that matches the permanent MAC address of one of the Ethernet PCI adapters currently in the system.

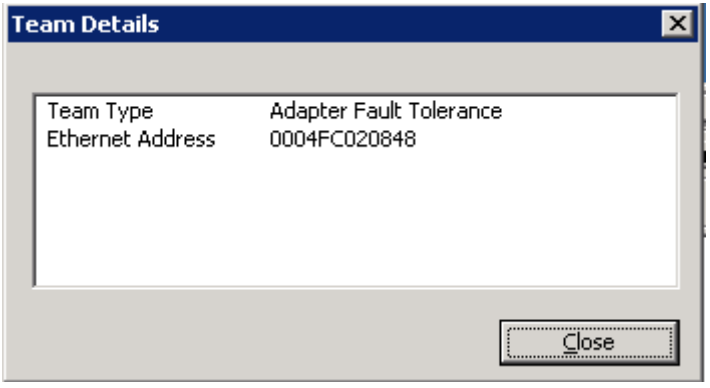
As a first step, verify that the team's current Ethernet address is identical to the permanent Ethernet address of one of the team members.

To verify the team Ethernet address

1. In the Network adapters node in Device Manager, right-click the target adapter team (not the adapter; see Figure B-4) and select **Properties**.
2. Select the **Settings** tab and then click on the **Details** button.

   The team Ethernet Address appears in the Team Details window. Figure B-16 shows an example. This address must match the address of one of the team's adapters. **Note this address for reference later in this procedure**.

Figure B-16. Obtaining the Team Ethernet Address



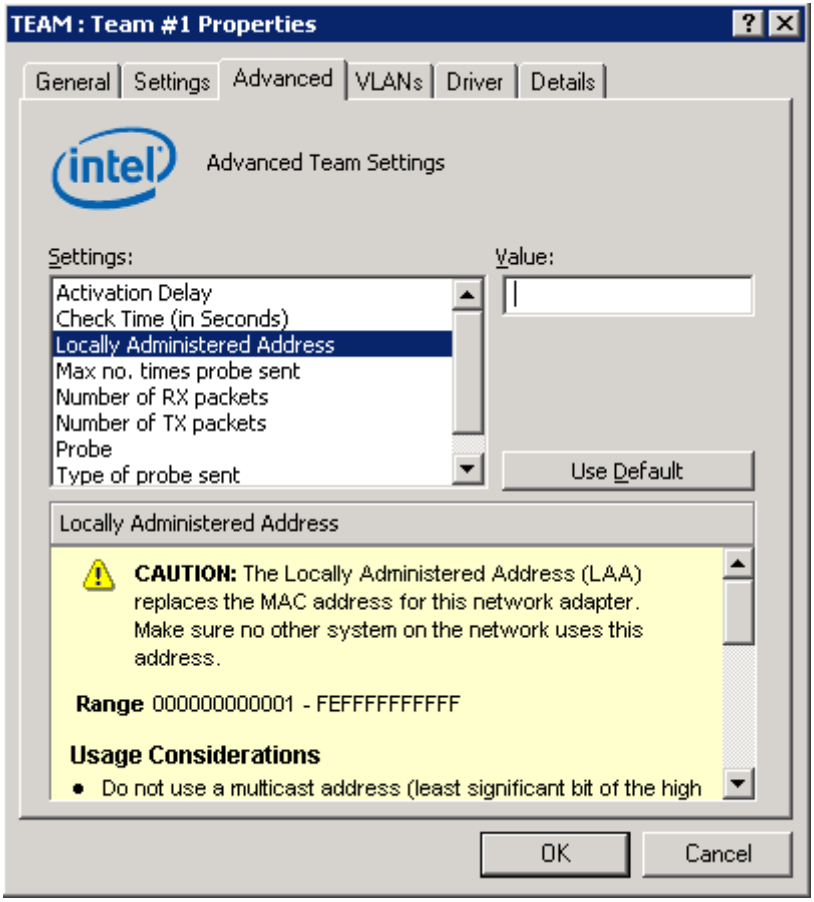
3. To obtain the permanent Ethernet address of an Ethernet PCI adapter, in the Network adapters node in Device Manager, right-click an adapter in the target team and select **Properties**.
4. Select the **Link Speed** tab and click the **Identify Adapter Details** button. The **Identify Adapter** dialog box appears. Figure B-1 shows an example.
5. Compare the value of **Permanent Ethernet Address** with the team Ethernet Address obtained in step 2 of this procedure. If the addresses match, no further action is needed.

If they do not match, then you must update the team's current Ethernet address.

To update the team Ethernet Address

1. In the Network adapters node in Device Manager, right-click the target team and select **Properties**.
2. Select the **Advanced** tab and under the Settings list, select **Locally Administered Address**. Figure B-17 shows an example.
3. In the Value field, enter the team Ethernet Address that you obtained in step 5 of the Ethernet address verification procedure. Click **OK**.

Figure B-17. Updating the Team Ethernet Address



NOTE

Changing the team mode forces the utility to update the Ethernet address of the team.

4. Again, right-click the team in the device tree in the left pane, and on the menu that appears, click **Change Team Mode**. Verify that the mode has been changed.
5. Click **OK** to process the procedure and to close. The update takes about 30 seconds to process.
6. Return to Device Manager and restore the team to its previous mode.
7. Click **Apply** to process and save the changes. Allow time for the update to process.

Removing an Ethernet Team

CAUTION

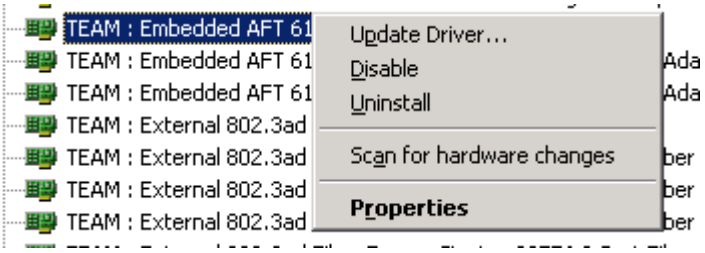
When you remove a team, you lose the connection to the network until you install and configure a new team.

If you assigned a specific IP address to the team, and if you are planning to configure a new team to use the same IP address, note the IP address of the team when you remove it. An assigned IP address is deleted when you remove the team.

To remove a team

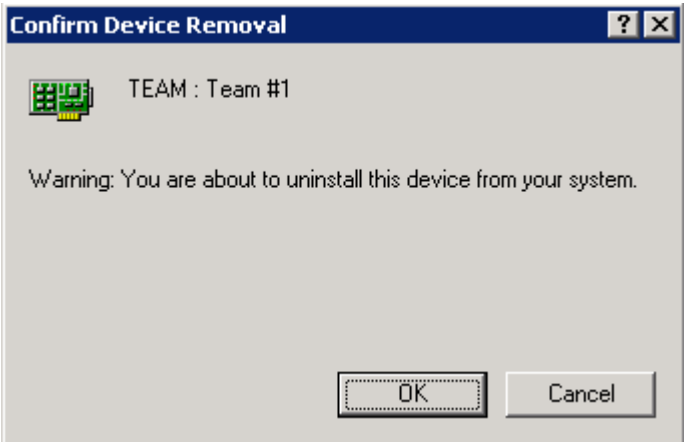
1. In the Network adapters node in Device Manager, right-click the target team and select **Uninstall**. Figure B-18 shows an example.

Figure B-18. Removing a Team of Ethernet PCI Adapters



2. In the Confirm Device Removal dialog box, click **OK** to uninstall the selected team. Figure B-19 shows an example.

Figure B-19. Confirmation Message: Removing a Team



Using Diagnostics

You can run connection, link, cable, and hardware diagnostics on your system's Ethernet infrastructure.

Running hardware diagnostic tests on the primary adapter in an AFT or SFT team stops network traffic until the secondary PCI adapter takes over. Running hardware diagnostics on the secondary adapter could reduce throughput. Running hardware diagnostics on an unteamed PCI adapter stops network traffic during the entire test.

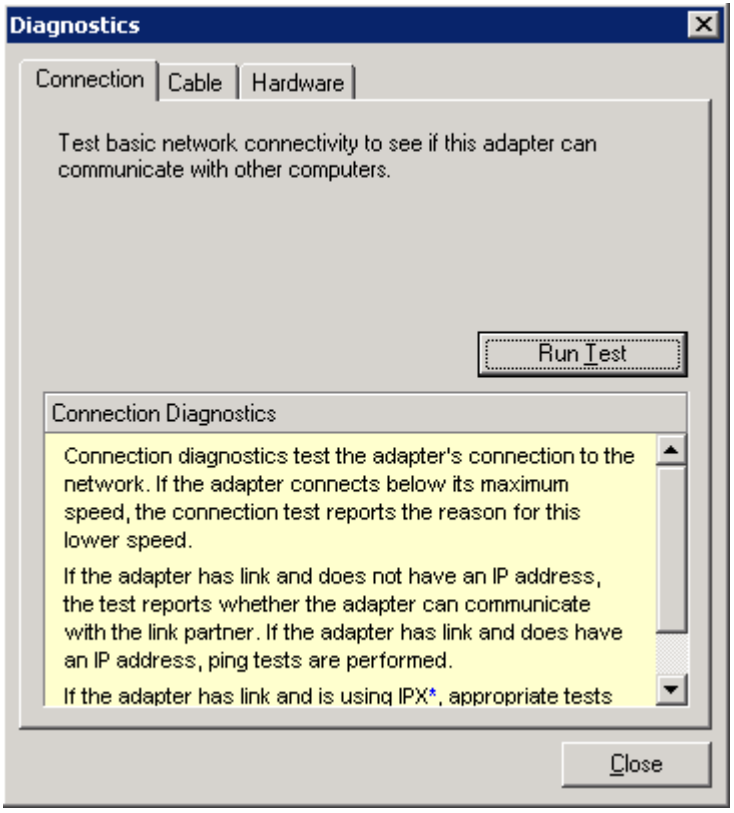
To start PROSet diagnostics

1. In the Network adapters node in Device Manager, right-click the target adapter and select **Properties**.
2. Select the **Link Speed** tab and click the **Diagnostics** button.
3. In the **Diagnostics** dialog box, click the **Connection**, **Cable**, or **Hardware** tab for the appropriate test (Figure B-20).
4. Click **Run Test**. The test results are displayed in the **Diagnostics** dialog box.

NOTE

Do not run the Connection test on a teamed adapter. It may return a false error report about not having valid IP information.

Figure B-20. Diagnostics

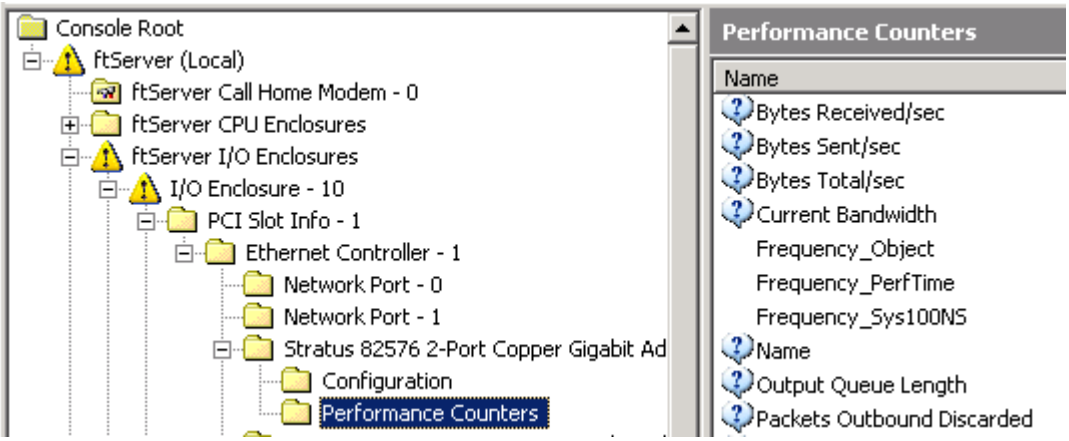

Diagnostics
Connection
Cable
Hardware
Test basic network connectivity to see if this adapter can communicate with other computers.
Run Test
Connection Diagnostics
Connection diagnostics test the adapter's connection to the network. If the adapter connects below its maximum speed, the connection test reports the reason for this lower speed.
If the adapter has link and does not have an IP address, the test reports whether the adapter can communicate with the link partner. If the adapter has link and does have an IP address, ping tests are performed.
If the adapter has link and is using IPX*, appropriate tests
Close

If you experience persistent network connectivity problems, try replacing the associated Ethernet PCI adapter(s). If that does not correct the problem, contact your authorized Stratus service representative.

Using ftSMC to Check Network Statistics

You can find network statistics for **unteamed** adapters in ftSMC. The statistics are located in **Performance Counters** under the **Ethernet Controller** node. Figure B-21 shows an example.

Figure B-21. Network Statistics in ftSMC



Renaming Ethernet Teams

When you create two or more teams on a new system or a system on which an IPL has just been performed, one of the teams may not have the name you assigned it. In the PROSet utility, the team name appears to be set correctly, but in Windows Network Connections, it is not the name you specified. Perform the following procedure to rename the incorrectly named team.

To rename a team

1. In the Network adapters node in Device Manager, right-click the target adapter and select **Properties**.
2. Select the **Settings** tab, click the **Modify Team** button and select the **Name** tab.
3. Enter the new team name in the Enter Team Name field and click **OK**. Click **OK** on the Settings tab.

   The new name appears in the Device Manager under the Network adapters node.

Index

A

action band, 3-7
active enclosures, 5-12
active RDR virtual disk (plex), 4-12
Active Upgrade, 1-1, 2-15
  preparing for, 3-13
ActiveService Network (ASN). *See* ASN
Adaptec SAS controller, 5-17
adapter team types, B-3
Add Physical Disk To RDR Virtual Disk
    command, 4-7
  error message, 4-9
administration. *See* system administration
Advanced Video Redirection (AVR), 1-3
alarm messages
  configuring system to send, 5-10
  sending over Internet only, 5-10
  sending over Internet with phone line as
      backup option, 5-10
  sending over phone line only, 5-10
  sending over phone line with Internet as
      backup option, 5-10
  system inventory, 5-11
ALB Ethernet adapter team, B-11
alerts. *See* alarm messages
application event logs, 2-8, 5-11
  saving, 2-9
ASN, 1-2
  configuration, 1-6
  features, 5-10
  system and PCI adapter integration, 1-5
automount behavior, 4-14

B

basic disks, 4-3
  converting dynamic to, 4-12
BIOS
  changing settings, 2-11, A-2
  determining version, 2-12
  Setup menus
    disabling boot monitoring, 5-15
  setup utilities
    starting, 2-11
BitLocker Drive Encryption, 1-4
boot disk
  requirements, 4-2
booting
  from backup system disk, 5-15
  from network drive, 2-15
  from spare system disk, 5-15
  monitoring process, 2-2
  stale disk, 4-24
bringup
  CPU element, 2-4

C

cache, enabling write, 4-10
call-home alarm messages. *See* alarm
    messages
Capacity property, 4-4
Clear MTBF command, 4-19
cloning RDR disks, 4-15
commands
  Add Physical Disk To RDR Virtual
      Disk, 4-7
  Clear MTBF, 4-19
    in RDR, 4-17
  Create RDR Virtual Disk, 4-5
  Delete RDR Configuration on Physical
      Disk, 4-13
  Deport Physical Disk from RDR Virtual
      Disk, 4-15
  operational states required for, 3-12
  Properties, 3-11
  Remove a Physical Disk from RDR Virtual
      Disk, 4-14
  Resynchronize This Physical Disk From
      RDR Virtual Disk, 4-22
  Set Cache Flush Interval, 4-11

Set Hard MTBF Threshold, 4-18
Set MTBF Faultcount Limit, 4-18
Set MTBF Threshold
in RDR, 4-17
Shut Down, 2-2
Stop Verify RDR Virtual Disk, 4-24
Verify RDR Virtual Disk, 4-24
components
determining failures, 5-6
labels, 5-8
locating, 5-7
status LEDs, 5-6
Computer Management
starting, 2-8
connection status of storage media in
ftSMC, 4-29
console tree of ftSMC, 3-7
context-sensitive help, 1-7
converting dynamic disks to basic RDR, 4-12
CPU elements, 3-12, 5-8
bringing up, 2-3
bringup options, 2-4
Dump and Go command, 5-14
memory dumps, 5-13
network connectivity when removing, B-1,
B-23
resynchronization, 2-3
states and actions, 3-12
CpuBringUpPolicy property, 2-4
CPU-I/O enclosures. *See* CPU elements *and*
I/O elements
Create RDR Virtual Disk command, 4-5
customer-replaceable unit failures, 5-12

D

data rate of Ethernet PCI adapters, B-7
data storage
dynamic disks, 4-26
fault tolerance, 4-1
debugging information files, 5-12
default gateways, VTM, 2-8
Defer CpuBoard Bringup, 2-4
Delete RDR Configuration on Physical Disk
command, 4-13
deleting RDR configurations
limitations, 4-13
Deport Physical Disk from RDR Virtual Disk
command, 4-15
deported disks, 4-15
desktop
enabling Remote Desktop, 2-5
Windows, 2-5
details pane of ftSMC, 3-7
device IDs
limitations, 5-8
locating components, 5-7
software components, 5-8
device paths
See device IDs
DevicePath property, 4-3, 4-30
DevicePathID property, 4-3, 4-30
devices
labels, 5-8
locating, 5-7
removing from, returning to, service, 2-15
diagnostics, B-29
disk management mirroring, 4-27
Disk node, 4-28
disks, 4-6
See also entries under RDR disk mirroring
and RDR virtual disks
active RDR, 4-12
backup, 4-15
duplex RDR, 4-3
finding in ftSMC, 4-3
finding internal in ftSMC, 4-29
mirroring in ftScalable Storage
systems, 4-29
replacing, 5-4
restrictions, 4-2
simplex, 4-3
status
Healthy, 5-4
Offline or Missing, 5-4
system boot, location of, 4-2
drive letters, 4-14
drivers
Board Instance, 5-13
elxstor.sys, 2-15
Emulex LightPulse Storport Miniport
driver, 2-15
Srabid, 2-4
tape, 5-17
dual device paths, software components, 5-8
Dump (NMI) button, 5-12

Dump and Go command
CPU element, 5-14
dump command, 5-12
dump files, 5-12
recovering, 5-13
DumpNumberOfFilesToSave property, 5-13
DumpQuickEnabled property, 5-13
dumps, 5-12
VTM, 5-14
duplex mode of Ethernet PCI adapters, B-7
DVD-RW drives, 2-12
dynamic disks, 4-4, 4-26
and RDR automatic disk expansion, 4-3
converting to basic, 4-12
Dynamic Host Configuration Protocol (DHCP), 1-3

E

elements. *See* CPU elements *and* I/O elements
elxstor.sys driver, 2-15
EMC storage enclosures
adapters in ftSMC, 4-28
Emulex LightPulse Storport Miniport driver, 2-15
Enable CpuBoard Bringup, 2-4
enabling write caching, 4-10
enclosures
active, 5-12
See also CPU elements *and* I/O elements
primary, 5-12
error icons, 5-6
Ethernet address
network filtering, B-21
updating, B-25
Ethernet PCI adapter teams
adding adapters to existing, B-24
assigning IP address, B-16, B-18
configuring primary adapters, B-12, B-22, B-25
configuring secondary adapters, B-12, B-22, B-25
configuring teams, B-6
configuring with third-party adapters, B-6
maximum number of teams, B-5
multicasting restriction, B-3
network filtering, B-21
removing adapters from existing, B-21
removing team, B-28
replacing primary adapter, B-25
restrictions and recommendations, B-5
restrictions when modifying existing, B-21
types, B-3
updating Ethernet (MAC) address, B-25
verifying configuration, B-16
Ethernet PCI adapters
adding to existing team, B-24
data rate, B-7
duplex mode, B-7
identifying, B-6
line speed, B-7
locating, B-6
network filtering, B-21
removing from team, B-21
Ethernet teams. *See* Ethernet PCI adapter teams
event logs
system, 5-11
events
log entries, 2-8, 5-11
reporting, 5-10
expanding all nodes, 3-6
explicit VLANs, B-5

F

failed component identification, 5-6
failover, 4-12
failures
CRUs, 5-12
determining component, 5-6
disk, 4-23, 5-3
mean time between (MTBF), 5-2
mirrored disks, 4-25
mirrored volumes, 4-26
replacing disks, 5-4
Stratus services, 2-11
system, 5-6
UPS, 2-14
FaultCountLimit property, 4-18
fault-resilient boot failure, 5-11
files
boot.ini
modifying, 5-16
debugging, 5-12
dump, 5-12
memory dump, 5-13
paging, 4-15

paging and RDR, 4-13
saving event log, 2-9
saving log, 2-10
system-critical, 4-2
Windows hotfix, 5-16
finding components, 5-7
flashing LEDs, 5-7
ftScalable Storage, 4-27
mirroring disks, 4-29
nodes, 4-27, 4-28
ftServer model
determining your system, 3-1
ftSMC
action band definition, 3-7
adding to MMC, 3-3, 3-4
console tree definition, 3-7
details pane definition, 3-7
inventory icons, 3-8
network statistics, B-30
running on remote computer, 3-3, 3-4
status bar definition, 3-7
unteamed adapters, network statistics, B-30
updating status of storage connection state, 4-29
ftSys Management Console. *See* ftSMC

G

GARP VLAN Registration Protocol (GVRP), B-5

H

hanging system, 2-2
hard MTBF, setting threshold, 4-18
hardware installation wizard, 5-5
headless mode, A-1
Healthy disk status, 5-4
Help in ftSMC
context-sensitive, 1-7
overview, 1-7
What's this?, 1-7
hotfixes
installing, 2-15
obtaining list, 5-16

I

I/O elements, 3-12, 5-8
active, 5-12
hot-plugging, 5-5
in details pane, 4-30
primary, 5-12
resynchronizing mirrored volumes, 4-26
resynchronizing RDR disks, 4-21
states and actions, 3-12
icons
dimmed folder, 3-8
dual monitor, 3-8
error, 3-9, 5-6
invalid configuration, 3-9
inventory, 3-8
magnifying glass, 3-8
no inventory found, 3-10
single monitor, 3-8
threshold warning, 3-10
tools, 3-8
warning, 5-6
yellow folder, 3-8
identifiers
device
limitations of device, 5-8
identifying a system model, 3-1
identifying components
Ethernet PCI adapters, B-6
flashing LEDs, 5-7
IMAPI service, enabling, 2-12
implicit VLANs, B-5
Initiate BringDown command
Op State required, 3-12
Initiate BringUp command
Op State required, 3-12
Initiate Diagnostics command
Op State required, 3-12
internal disks
configuration guidelines, 4-2
in ftSMC, 4-27
mirroring, 4-2
unsafe removal error message, 4-14, 4-23, 5-3
internal storage enclosures
in details pane, 4-30
invalid component configurations, 3-9

IP address
Ethernet PCI adapter team, B-16, B-18
VLAN, B-16, B-18
UPS configuration, 2-14
VTMs, 2-8
IP multicasting, B-3

L

labels
on components, 5-8
LEDs
component status, 5-6
flashing to find components, 5-7
line speed of Ethernet PCI adapters, B-7
locating components
Ethernet PCI adapters, B-6
flashing LEDs, 5-7
log files, 2-8
Logical to Physical Mapping node, 4-29
login
enabling multiple remote sessions, A-2
LUN, 4-3
LunVerifyInterval property, 4-24

M

MAC address
network filtering, B-21
updating, B-25
mean time between failures. *See* MTBF
memory snapshot
Dump and Go feature, 5-13
metadata, 4-3
space requirement, 4-10
Microsoft Windows. *See* Windows
mirroring
and failed volumes, 4-26
disks in internal storage, 4-3
recovering non-RDR disk, 5-4
recovering RDR disk, 4-23, 5-3
status
Healthy, 5-4
Offline or Missing, 5-4
synchronizing, 4-26
volumes, 4-26
missing Ethernet PCI adapter, B-23
MMC
adding snap-in to, 3-3, 3-4
running, 3-5
modems
powering while online, 2-4
monitoring
disk resynchronization, 4-21
services, 2-10
system
remotely, 1-2, 3-2
MTBF
clearing, 4-19
Faultcount Limit property, 4-18
managing, 5-2
setting hard threshold, 4-18
setting soft threshold, 4-19
statistics, 5-2
threshold
changing, 5-2
values, 5-2
multicasting, B-3
multiple Windows login sessions
enabling, A-2

N

NMI button, 5-12
nodes
Disk, 4-28
expanding, 3-6
Logical to Physical Mapping, 4-29
SCSI Port Duplex Driver - Sradisk_Driver, 4-5
Slot, 4-28
Storage Enclosure, 4-27
nonmaskable interrupts (NMI)
with VTMs, 5-14

O

offline component identification, 5-6
Offline or Missing disk status, 5-4
Op State status
Initiate BringDown command, 3-12
Initiate BringUp command, 3-12
Initiate Diagnostics command, 3-12
Set Priority, 3-12
optimizing system performance, 4-10

P

paging files, 4-15
PCI adapters
  EMC storage systems, 4-28
  Ethernet teams, 1-6
  ftScalable Storage system, 4-28
  managing Ethernet, B-1
pedestal systems
  locations of elements, 4-30
plexes, 4-3
  active RDR, 4-12
power button
  enabling, 2-2
powering down system, 2-2
primary elements, 3-12
  switching, 3-13
primary enclosures, 3-12, 5-12
  switching, 3-13
primary Ethernet PCI adapter
  configuring, B-12, B-22, B-25
  replacing, B-25
procedures
  adding ftSMC to MMC, 3-3, 3-4
  archiving log files, 2-9
  booting from spare disk, 5-15
  changing IP address for UPS, 2-14
  configuring a UPS, 1-6
  deleting RDR configuration on a physical disk, 4-13
  deporting physical disk from RDR virtual disk, 4-16
  determining component failure, 5-6
  enabling IMAPI, 2-12
  enabling IMAPI for DVD-RW reading and writing, 2-12
  enabling read-load balancing (globally), 4-11
  enabling read-load balancing, single disk, 4-11
  enabling Remote Desktop, 2-5
  enabling write caching, 4-10
  obtaining list of Windows hotfixes, 5-16
  prioritizing resynchronization for all RDR disks, 4-25
  prioritizing resynchronization for individual RDR disks, 4-25
  recovering
    when Windows hangs, 5-9
  recovering an offline non-RDR disk, 5-4
  recovering an RDR disk, 4-23, 5-3
  removing physical disk from RDR virtual disk, 4-15
  replacing a failed disk, 5-4
  replacing a failed physical RDR disk, 4-23
  resynchronizing RDR data disks, 4-22
  saving log files, 2-9, 2-10
  setting size of application and system event logs, 2-9
  setting the interval for automatic RDR disk verification, 4-24
  starting BIOS setup utilities, 2-11
  verifying an RDR disk, 4-24
Properties command, 3-11
PROSet utility
  removing entry for missing adapter, B-23
  using from remote system, B-3

R

rack-mounted systems
  locations of elements, 4-30
RDR disk mirroring, 1-5, 4-6
  automatic disk configuration, 4-6
  boot volume with disk management tool, 4-27
  breaking a physical disk from a virtual disk, 4-17
  cloning, 4-15
  converting disks, 4-12
  deleting configuration, 4-13
  deporting physical disks, 4-15
  disk resynchronization, 4-21
  dynamic disks, 4-12
  metadata, 4-3
  monitoring resynchronization, 4-21
  recovering disk, 4-23, 5-3
  removing physical disks, 4-14
RDR virtual disks
  active plex, 4-12
  adding a physical disk to, error message, 4-9
  automatic expansion, 4-3
  automatic verification, 4-24
  backup, 4-15
  booting from spare (deported), 4-17
  breaking, 4-17
  Capacity property, 4-4

cloning, 4-15
creating spare bootable, 4-16
deleting data from, 4-14
deleting RDR configuration, 4-13
deported, 4-15
duplexed, 4-3
failed during resynchronization, 4-10
finding in ftSMC, 4-29
finding physical disks of in ftSMC, 4-3
invalid procedures and error messages, 4-6
mirrored, 4-3
physical disk and virtual disk capacity, 4-4
read-load balancing, 4-11
replacing a failed, 4-23
resynchronization priority, 4-25
resynchronizing blanks, 4-22
reusing stored-data disks, 4-20
settings parameters, 4-5
simplex, 4-3
verifying mirror integrity, 4-23
volume mirroring, 4-3
write caching, 4-10
read-load balancing, 4-11
reboot
delayed, 5-9
receive load balancing, disabling, B-11
Remote Desktop
enabling, 2-5
enabling multiple login sessions, A-2
Remove a Physical Disk from RDR Virtual Disk command, 4-14
replacing disks, 5-4
Reserved VTM IP address, 2-8
resynchronization
CPU elements, 2-3
RDR disks, 4-21
Resynchronize This Physical Disk From RDR Virtual Disk command, 4-22

S

Safe Mode system recovery, 5-14
scheduling CPU bringup, 2-3
SCSI Port Duplex Driver - Sradisk_Driver node, 4-5
setting disk parameters, 4-5
secondary elements, 3-12
switching, 3-13
secondary enclosures, 3-12
switching, 3-13
secondary Ethernet PCI adapters, configuring, B-12, B-22, B-25
Send Alarms By property, 5-10
services
listing installed Stratus, 2-10
monitoring, 2-10
system, 1-4
starting and stopping, 1-4
Set Cache Flush Interval command, 4-11
Set Hard MTBF Threshold command, 4-18
Set MTBF Faultcount Limit command, 4-18
Set MTBF Threshold command
in RDR, 4-17
Set Priority command
Op State required, 3-12
Set Soft MTBF Threshold command, 4-19
Shut Down command, 2-2
shutting down system, 2-2
without logon, 2-2
Slot node, 4-28
snap-ins
adding ftSMC to MMC, 3-3, 3-4
SNMP traps, 2-14
soft MTBF, setting threshold, 4-19
stale disk, 4-24
Start Slot Identification command, 5-7
static IP addresses for the VTM console, 2-7
status bar
ftSMC, 3-7
status of disks
Healthy, 5-4
mirrors, 4-23, 5-3
Offline or Missing, 5-4
Stop Slot Identification command, 5-7
Stop Verify RDR Virtual Disk command, 4-24
Storage Enclosure node, 4-27
storage enclosures
labels, 5-8
storage, optional external, 4-27
subnet masks
VTMs, 2-8
switch (network)
configuring for VLANs, B-5
synchronizing mirrors, 4-26
system
delayed reboot, 5-9
determining model, 3-1

enabling power button, 2-2
hang time, 2-2
inventory
alarm messages, 5-11
icons, 3-8
performance optimization, 4-10
powering down, 2-2
remote monitoring, 1-2
starting up, 2-2
unbootable, 5-17
system administration tools, 1-1
system boot disk
requirements, 4-2
system disks
mirroring required, 4-25
system event logs (SELs), 2-9, 5-10, 5-11
saving, 2-9
setting maximum size, 2-9
Windows, 2-8
system power button, 2-2
system recovery
booting from spare disk, 5-15
Safe Mode, 5-14
system shutdown without logon, 2-2

T

tape drive, 5-17
team types, B-3
teaming overview, B-3
teams. *See* Ethernet PCI adapter teams
thresholds
changing MTBF, 5-2
warning icon, 3-9
tools for system administration, 1-1
traps, SNMP, 2-14
troubleshooting PCI adapters
diagnostic tests, B-29
turning off system power, 2-2

U

unbootable system, 5-17
uninterruptible power supply. *See* UPS
Unsafe removal of device message, 4-14, 4-23, 5-3
UPS
configuring, 1-6, 2-13
connecting to, 2-14
updating IP address, 2-14

V

Verify RDR Virtual Disk command, 4-24
viewing all nodes, 3-6
Virtual LANs. *See* VLANs
Virtual Technician Module. *See* VTM
VLANs, B-4
assigning IP address, B-16, B-18
explicit, B-5
GARP VLAN Registration Protocol (GVRP), B-5
implicit, B-5
verifying configuration, B-16
VLAN ID, B-5, B-15
volume mirroring, 4-26
VTM
dumps, 5-14
managing Administrator account, 2-6
overview, 1-3
VTM console
assigning static IP address, 2-7
logging in, 2-7
overview, 1-3
starting and stopping system, 2-6

W

warning icons, 5-6
What's this? Help
accessing, 1-7
for details pane properties, 3-7
Windows
accessing desktop, 2-5
not responding, 5-9
obtaining list of hotfixes, 5-16
Windows Device Manager, disabling devices, 2-15
Windows hotfixes, installing, 2-15
Windows Server 2008 system tape driver, 5-17
Windows updates, installing, 2-15
wizard
Add Physical Disk to RDR Virtual Disk, 4-7
hardware installation, 5-5
write caching on RDR virtual disks, 4-10